Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/001398

International filing date: 01 February 2005 (01.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-125196
Filing date: 21 April 2004 (21.04.2004)

Date of receipt at the International Bureau: 31 March 2005 (31.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/JP2005/001398

04. 2. 2005

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

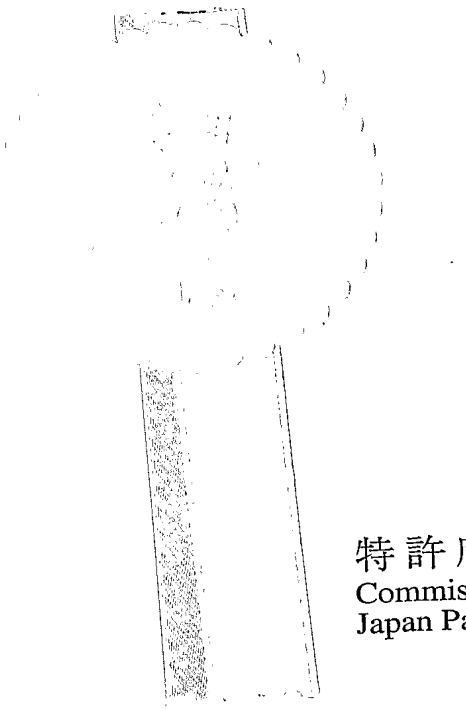
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　４月２１日

出願番号
Application Number: 特願２００４－１２５１９６

[ST. 10/C]: [ＪＰ２００４－１２５１９６]

出願人
Applicant(s): 松下電器産業株式会社



２００５年　３月１８日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３０２４２９８

【書類名】　特許願
【整理番号】　2048160137
【提出日】　平成16年 4月21日
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　原田　俊治
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　井藤　好克
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　中野　稔久
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　横田　薫
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　高橋　潤
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100097445
　【弁理士】
　【氏名又は名称】　岩橋　文雄
【選任した代理人】
　【識別番号】　100103355
　【弁理士】
　【氏名又は名称】　坂口　智康
【選任した代理人】
　【識別番号】　100109667
　【弁理士】
　【氏名又は名称】　内藤　浩樹
【手数料の表示】
　【予納台帳番号】　011305
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9809938

【書類名】特許請求の範囲
【請求項１】
コンテンツを保持する第１の装置から第２の装置へコンテンツを移動する、もしくは、第２の装置から第１の装置へコンテンツを移動することが可能な著作権保護システムであって、
前記第１の装置は、第１の暗号化コンテンツ、及び、第１の暗号化コンテンツと関連する第２の暗号化コンテンツを記録するコンテンツ記録部と、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを復号するためのコンテンツ鍵を記録する鍵記録部と、前記コンテンツ鍵へのアクセスを制御する鍵制御部とを備え、
前記第２の装置は、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを記録するコンテンツ記録部と、前記コンテンツ鍵を記録する鍵記録部とを備え、
前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記第１の装置から前記第２の装置に移動する際、前記第１の装置の鍵制御部による制御の下で、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を、前記第２の装置の鍵記録部に記録し、前記第１の装置のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記第２の装置のコンテンツ記録部に記録することを特徴とする著作権保護システム。
【請求項２】
前記第１の装置の鍵制御部は、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を利用不可能な状態にして、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を、前記第２の装置の鍵記録部に記録することを特徴とする請求項１記載の著作権保護システム。
【請求項３】
前記第１の装置の鍵制御部は、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を消去し、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を、前記第２の装置の鍵記録部に記録することを特徴とする請求項１記載の著作権保護システム。
【請求項４】
前記第１の装置の鍵制御部は、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を利用不可能な状態にして、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を、前記第２の装置の鍵記録部に記録し、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を消去することを特徴とする請求項１記載の著作権保護システム。
【請求項５】
前記第１の装置は、さらに認証部を備え、前記第２の装置は、さらに認証部を備え、
前記第１の装置の認証部は、前記第２の装置の認証部との間で認証処理を行い、認証処理が成功したときに、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を、前記第２の装置の鍵記録部に記録することを特徴とする請求項１記載の著作権保護システム。
【請求項６】
前記第１の装置は、さらに、認証部、および、鍵暗号部を備え、前記第２の装置は、さらに認証部、および、鍵暗号部を備え、
前記第１の装置の認証部は、前記第２の装置の認証部との間で認証処理を行い、認証処理が成功したときに、前記第１の装置の認証部と、前記第２の装置の認証部は、それぞれ、セッション鍵を生成し、前記第１の装置の鍵暗号部は、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を前記セッション鍵で暗号化して第２の装置に送り、前記第２の装置の鍵暗号部は、受け取った暗号化されたコンテンツ鍵を前記セッション鍵で復号し、復号したコンテンツ鍵を前記第２の装置の鍵記録部に記録することを特徴とする請求項１記載の著作権保護システム。
【請求項７】
前記第１の装置は、さらに、コピー制御情報を記録するコピー制御情報記録部と、前記コピー制御情報に基づいて、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記第１の装置から前記第２の装置に移動することが認められているか否か

を判定する判定部を備えたことを特徴とする請求項１記載の著作権保護システム。
【請求項８】
前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記第２の装置から前記第１の装置に移動する際、前記第１の装置の鍵制御部による制御の下で、前記第２の装置の鍵記録部に記録しているコンテンツ鍵を、前記第１の装置の鍵記録部に記録し、前記第２の装置のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記第１の装置のコンテンツ記録部に記録することを特徴とする請求項１記載の著作権保護システム。
【請求項９】
前記第１の装置の鍵制御部は、前記第１の装置の鍵記録部へ記録するコンテンツ鍵を利用不可能な状態にして、前記第２の装置の鍵記録部に記録しているコンテンツ鍵を、前記第１の装置の鍵記録部に記録し、前記第２の装置の鍵記録部に記録しているコンテンツ鍵を消去し、前記第１の装置の鍵記録部へ記録するコンテンツ鍵を利用可能な状態にすることを特徴とする請求項８記載の著作権保護システム。
【請求項１０】
コンテンツを、コンテンツ鍵で暗号化したものを第１の暗号化コンテンツとし、前記コンテンツを変換して得られた変換コンテンツを、前記コンテンツ鍵で暗号化したものを第２の暗号化コンテンツとすることを特徴とする請求項１記載の著作権保護システム。
【請求項１１】
前記第１の装置が、記録再生装置であり、前記第２の装置が、前記記録再生装置により、データの読み書きが可能な可搬媒体であることを特徴とする請求項１記載の著作権保護システム。
【請求項１２】
コンテンツを可搬媒体へ移動する、もしくは、可搬媒体からコンテンツを移動することが可能な記録再生装置であって、
　第１の暗号化コンテンツ、及び、第１の暗号化コンテンツと関連する第２の暗号化コンテンツを記録するコンテンツ記録部と、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを復号するためのコンテンツ鍵を記録する鍵記録部と、前記コンテンツ鍵へのアクセスを制御する鍵制御部とを備え、
　前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記記録再生装置から前記可搬媒体に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記記録再生装置の鍵記録部に記録しているコンテンツ鍵を、前記可搬媒体に記録し、前記第１の装置のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記可搬媒体に記録することを特徴とする記録再生装置。
【請求項１３】
前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記可搬媒体から前記記録再生装置に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記可搬媒体の鍵記録部に記録しているコンテンツ鍵を、前記記録再生装置の鍵記録部に記録し、前記可搬媒体のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記記録再生装置のコンテンツ記録部に記録することを特徴とする請求項１２記載の記録再生装置。
【請求項１４】
記録再生装置へコンテンツを移動する、もしくは、記録再生装置からコンテンツを移動することが可能な可搬媒体であって、
　前記可搬媒体は、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを記録するコンテンツ記録部と、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを復号するためのコンテンツ鍵を記録する鍵記録部とを備え、
　前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記記録再生装置から可搬媒体に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記記録再生装置の鍵記録部に記録しているコンテンツ鍵を、前記可搬媒体の鍵記録部に記録

し、前記記録再生装置のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記可搬媒体のコンテンツ記録部に記録することを特徴とする可搬媒体。

【請求項１５】

前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記可搬媒体から前記記録再生装置に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記可搬媒体の鍵記録部に記録しているコンテンツ鍵を、前記記録再生装置の鍵記録部に記録し、前記可搬媒体のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記記録再生装置のコンテンツ記録部に記録することを特徴とする請求項１４記載の可搬媒体。

【請求項１６】

コンテンツを保持する第１の装置から第２の装置へコンテンツを移動する、もしくは、第２の装置から第１の装置へコンテンツを移動することが可能な著作権保護システムであって、

前記第１の装置は、第１の暗号化コンテンツ、及び、第１の暗号化コンテンツと関連する第２の暗号化コンテンツを記録するコンテンツ記録部と、前記第１の暗号化コンテンツを復号するための第１のコンテンツ鍵、及び、前記第２の暗号化コンテンツを復号するための第２コンテンツ鍵を記録する鍵記録部と、前記第１のコンテンツ鍵、及び、第２のコンテンツ鍵へのアクセスを制御する鍵制御部とを備え、

前記第２の装置は、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを記録するコンテンツ記録部と、前記第１のコンテンツ鍵、もしくは、第２のコンテンツ鍵を記録する鍵記録部とを備え、

前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記第１の装置から前記第２の装置に移動する際、前記第１の装置の鍵制御部による制御の下で、前記第１の装置の鍵記録部に記録している第１のコンテンツ鍵、もしくは第２のコンテンツ鍵を、前記第２の装置の鍵記録部に記録し、前記第１の装置のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記第２の装置のコンテンツ記録部に記録することを特徴とする著作権保護システム。

【請求項１７】

前記第１の装置の鍵制御部は、前記第１の装置の鍵記録部に記録している第１のコンテンツ鍵、並びに、第２のコンテンツ鍵を利用不可能な状態にして、前記第１の装置の鍵記録部に記録している第１のコンテンツ鍵、もしくは第２のコンテンツ鍵を、前記第２の装置の鍵記録部に記録し、前記第２の装置の鍵記録部に記録した第１のコンテンツ鍵、もしくは、第２のコンテンツ鍵を、前記第１の装置の鍵記録部から消去することを特徴とする請求項１６記載の著作権保護システム。

【請求項１８】

前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記第２の装置から前記第１の装置に移動する際、前記第１の装置の鍵制御部による制御の下で、前記第２の装置の鍵記録部に記録している第１のコンテンツ鍵、もしくは第２のコンテンツ鍵を、前記第１の装置の鍵記録部に記録し、前記第２の装置のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記第１の装置のコンテンツ記録部に記録することを特徴とする請求項１６記載の著作権保護システム。

【請求項１９】

前記第１の装置の鍵制御部は、前記第１の装置の鍵記録部へ記録する第１のコンテンツ鍵、もしくは、第２のコンテンツ鍵を利用不可能な状態にして、前記第２の装置の鍵記録部に記録している第１のコンテンツ鍵、もしくは、第２のコンテンツ鍵を、前記第１の装置の鍵記録部に記録し、前記第２の装置の鍵記録部に記録している第１のコンテンツ鍵、もしくは第２のコンテンツ鍵を消去し、前記第１の装置の鍵記録部へ記録する第１のコンテンツ鍵、もしくは第２のコンテンツ鍵を利用可能な状態にすることを特徴とする請求項１８記載の著作権保護システム。

【書類名】明細書
【発明の名称】記録再生装置、可搬媒体、及び著作権保護システム
【技術分野】
【０００１】
本発明は、コンテンツの不正利用防止を目的とした記録再生装置、及び可搬媒体を含む著作権保護システムに関し、特に、不正利用を防止しつつユーザの利便性を高める技術に関する。
【背景技術】
【０００２】
近年、ＢＳデジタル放送や地上デジタル放送の開始に伴い、映画等のデジタルコンテンツが広く配信されるようになってきている。デジタルコンテンツ（以下、コンテンツ）は複製が容易であるため、インターネットやその他の媒体を介した海賊行為、並びに複製コンテンツの再配信などの不正行為に対する懸念が高まっており、これら不正行為に対抗（コンテンツを保護）するための技術開発が進められている。
【０００３】
このようなコンテンツの保護技術に関する規格として、例えば、ＤＴＣＰ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ）がある。ＤＴＣＰは、コンテンツをデジタル転送する際に、コンテンツを暗号化するなどして不正コピーを防止する技術である。ＤＴＣＰのようなコンテンツ保護技術においては、コンテンツに、「Ｃｏｐｙ　Ｎｏ　Ｍｏｒｅ」、「Ｃｏｐｙ　Ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」等のコピー制御情報（ＣＣＩ：Ｃｏｐｙ　Ｃｏｎｔｒｏｌ　Ｉｎｆｏｒｍａｔｉｏｎ）を付与する。「Ｃｏｐｙ　Ｎｏ　Ｍｏｒｅ」はコンテンツのコピーが禁止されていることを表し、「Ｃｏｐｙ　Ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」はコンテンツのコピーが１回だけ許されていることを表す。従って、コピー制御情報として「Ｃｏｐｙ　Ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」が付与されたコンテンツをコピーすると、コピーによって新たに得られたコンテンツには、コピー制御情報として「Ｃｏｐｙ　Ｎｏ　Ｍｏｒｅ」が付与される。
【０００４】
一方で、コピー制御情報として「Ｃｏｐｙ　Ｎｏ　Ｍｏｒｅ」が付与されたコンテンツであっても、他の記録媒体、あるいは他の装置へ移動させたいという要望がある。例えば、デジタルテレビに内蔵されているＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）に記録されているコンテンツをＤＶＤ－ＲＡＭに移動させて保存版として保管しておきたいような場合である。この際（ＨＤＤからＤＶＤ－ＲＡＭにコンテンツを移動させた場合）、デジタルテレビ内蔵ＨＤＤの当該コンテンツは、当然、再生できない状態にされなければならない。例えば、内蔵ＨＤＤからＤＶＤ－ＲＡＭにコンテンツをコピーした後に、内蔵ＨＤＤに記録されているコンテンツを消去するなどしてコンテンツを無効化する、すなわちコンテンツを利用できない状態にする方法などが考えられる。しかしながら、コンテンツの移動に先立ってデジタルテレビから内蔵ＨＤＤを取り出し、これをパーソナルコンピュータに接続してバックアップを作成し、コンテンツを移動した後にバックアップしておいたデータを内蔵ＨＤＤに戻すという操作が行われると、コンテンツを何度でも移動できることになり、事実上不正コピーを防止することができなくなる。
【０００５】
また、内蔵のＨＤＤからＤＶＤ－ＲＡＭにコンテンツをコピーした後、内蔵ＨＤＤに記録されているコンテンツを消去する方法では、コピーした後に、記録再生装置から記録媒体を不正に引き抜かれた場合に、記録再生装置の内蔵ＨＤＤと、ＤＶＤ－ＲＡＭの両方にコンテンツが存在し、不正コピーを防止できなくなる。
【０００６】
また、コンテンツの移動中の電源断などの原因により、移動元と移動先のコンテンツが共に損なわれ、コンテンツとして利用できなくなることは、コンテンツを利用するユーザにとっては不便である。さらに、このようにして利用できなくなったコンテンツを再度入手するために出費が必要な場合には経済的な損失も発生する。

【０００７】
上記課題を解決するための従来技術として、不正コピーを防止しながら、コンテンツの喪失を招くことなく、コンテンツの移動を可能にする技術が特許文献１に開示されている。

【特許文献１】特開２００３－２２８５２２号公報
【非特許文献１】「現代暗号理論」、池野信一、小山謙二、電子通信学会
【非特許文献２】「暗号理論入門」、岡本栄司、共立出版株式会社

【発明の開示】
【発明が解決しようとする課題】
【０００８】
しかしながら、移動元のコンテンツが高画質コンテンツであり、コンテンツのサイズに比べて、移動先の記録容量が小さい場合には、コンテンツの移動前に、その画質を劣化させるなどしてサイズを小さく圧縮変換してから移動を行うのが通例であるが、前記構成のようにコンテンツを消去するなどして移動元のコンテンツを無効化する場合、圧縮変換された（画質の劣化した）コンテンツだけがユーザの下に残ることになる。すなわち、再び記録容量の大きな内蔵ＨＤＤへコンテンツを戻す（移動する）場合であっても、画質の劣化されたコンテンツを高画質コンテンツへ変換することは不可能であり、元々の高画質コンテンツは復元されないため、これはコンテンツを利用するユーザの利便性が損なわれることにつながる。
【０００９】
本発明は、前記課題を解決するものであって、不正コピーを防止しながら、コンテンツの喪失を招くことなくコンテンツの移動を可能にして、さらに、サイズを小さくする圧縮変換後であっても、当該コンテンツを移動元に戻す場合には、元々の高画質コンテンツの復元を可能にする記録再生装置、並びに可搬媒体を含む著作権保護システムの提供を目的とする。
【課題を解決するための手段】
【００１０】
本発明は、コンテンツを保持する第１の装置から第２の装置へコンテンツを移動する、もしくは、第２の装置から第１の装置へコンテンツを移動することが可能な著作権保護システムであって、前記第１の装置は、第１の暗号化コンテンツ、及び、第１の暗号化コンテンツと関連する第２の暗号化コンテンツを記録するコンテンツ記録部と、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを復号するためのコンテンツ鍵を記録する鍵記録部と、前記コンテンツ鍵へのアクセスを制御する鍵制御部とを備え、前記第２の装置は、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを記録するコンテンツ記録部と、前記コンテンツ鍵を記録する鍵記録部とを備え、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記第１の装置から前記第２の装置に移動する際、前記第１の装置の鍵制御部による制御の下で、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を、前記第２の装置の鍵記録部に記録し、前記第１の装置のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記第２の装置のコンテンツ記録部に記録することを特徴とする。
【００１１】
また、前記第１の装置の鍵制御部は、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を利用不可能な状態にして、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を、前記第２の装置の鍵記録部に記録することを特徴とする。
【００１２】
また、前記第１の装置の鍵制御部は、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を消去し、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を、前記第２の装置の鍵記録部に記録することを特徴とする。
【００１３】

また、前記第１の装置の鍵制御部は、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を利用不可能な状態にして、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を、前記第２の装置の鍵記録部に記録し、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を消去することを特徴とする。

【００１４】

また、前記第１の装置は、さらに認証部を備え、前記第２の装置は、さらに認証部を備え、前記第１の装置の認証部は、前記第２の装置の認証部との間で認証処理を行い、認証処理が成功したときに、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を、前記第２の装置の鍵記録部に記録することを特徴とする。

【００１５】

また、前記第１の装置は、さらに、認証部、および、鍵暗号部を備え、前記第２の装置は、さらに認証部、および、鍵暗号部を備え、前記第１の装置の認証部は、前記第２の装置の認証部との間で認証処理を行い、認証処理が成功したときに、前記第１の装置の認証部と、前記第２の装置の認証部は、それぞれ、セッション鍵を生成し、前記第１の装置の鍵暗号部は、前記第１の装置の鍵記録部に記録しているコンテンツ鍵を前記セッション鍵で暗号化して第２の装置に送り、前記第２の装置の鍵暗号部は、受け取った暗号化されたコンテンツ鍵を前記セッション鍵で復号し、復号したコンテンツ鍵を前記第２の装置の鍵記録部に記録することを特徴とする。

【００１６】

また、前記第１の装置は、さらに、コピー制御情報を記録するコピー制御情報記録部と、前記コピー制御情報に基づいて、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記第１の装置から前記第２の装置に移動することが認められているか否かを判定する判定部を備えたことを特徴とする。

【００１７】

また、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記第２の装置から前記第１の装置に移動する際、前記第１の装置の鍵制御部による制御の下で、前記第２の装置の鍵記録部に記録しているコンテンツ鍵を、前記第１の装置の鍵記録部に記録し、前記第２の装置のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記第１の装置のコンテンツ記録部に記録することを特徴とする。

【００１８】

また、前記第１の装置の鍵制御部は、前記第１の装置の鍵記録部へ記録するコンテンツ鍵を利用不可能な状態にして、前記第２の装置の鍵記録部に記録しているコンテンツ鍵を、前記第１の装置の鍵記録部に記録し、前記第２の装置の鍵記録部に記録しているコンテンツ鍵を消去し、前記第１の装置の鍵記録部へ記録するコンテンツ鍵を利用可能な状態にすることを特徴とする。

【００１９】

また、コンテンツを、コンテンツ鍵で暗号化したものを第１の暗号化コンテンツとし、前記コンテンツを変換して得られた変換コンテンツを、前記コンテンツ鍵で暗号化したものを第２の暗号化コンテンツとすることを特徴とする。

【００２０】

また、前記第１の装置が、記録再生装置であり、前記第２の装置が、前記記録再生装置により、データの読み書きが可能な可搬媒体であることを特徴とする。

【００２１】

また、コンテンツを可搬媒体へ移動する、もしくは、可搬媒体からコンテンツを移動することが可能な記録再生装置であって、第１の暗号化コンテンツ、及び、第１の暗号化コンテンツと関連する第２の暗号化コンテンツを記録するコンテンツ記録部と、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを復号するためのコンテンツ鍵を記録する鍵記録部と、前記コンテンツ鍵へのアクセスを制御する鍵制御部とを備え、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記記録再生

装置から前記可搬媒体に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記記録再生装置の鍵記録部に記録しているコンテンツ鍵を、前記可搬媒体に記録し、前記第１の装置のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記可搬媒体に記録することを特徴とする。

【００２２】

また、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記可搬媒体から前記記録再生装置に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記可搬媒体の鍵記録部に記録しているコンテンツ鍵を、前記記録再生装置の鍵記録部に記録し、前記可搬媒体のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記記録再生装置のコンテンツ記録部に記録することを特徴とする。

【００２３】

また、記録再生装置へコンテンツを移動する、もしくは、記録再生装置からコンテンツを移動することが可能な可搬媒体であって、前記可搬媒体は、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを記録するコンテンツ記録部と、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを復号するためのコンテンツ鍵を記録する鍵記録部とを備え、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記記録再生装置から可搬媒体に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記記録再生装置の鍵記録部に記録しているコンテンツ鍵を、前記可搬媒体の鍵記録部に記録し、前記記録再生装置のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記可搬媒体のコンテンツ記録部に記録することを特徴とする。

【００２４】

また、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記可搬媒体から前記記録再生装置に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記可搬媒体の鍵記録部に記録しているコンテンツ鍵を、前記記録再生装置の鍵記録部に記録し、前記可搬媒体のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記記録再生装置のコンテンツ記録部に記録することを特徴とする。

【００２５】

また、コンテンツを保持する第１の装置から第２の装置へコンテンツを移動する、もしくは、第２の装置から第１の装置へコンテンツを移動することが可能な著作権保護システムであって、前記第１の装置は、第１の暗号化コンテンツ、及び、第１の暗号化コンテンツと関連する第２の暗号化コンテンツを記録するコンテンツ記録部と、前記第１の暗号化コンテンツを復号するための第１のコンテンツ鍵、及び、前記第２の暗号化コンテンツを復号するための第２コンテンツ鍵を記録する鍵記録部と、前記第１のコンテンツ鍵、及び、第２のコンテンツ鍵へのアクセスを制御する鍵制御部とを備え、前記第２の装置は、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを記録するコンテンツ記録部と、前記第１のコンテンツ鍵、もしくは、第２のコンテンツ鍵を記録する鍵記録部とを備え、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記第１の装置から前記第２の装置に移動する際、前記第１の装置の鍵制御部による制御の下で、前記第１の装置の鍵記録部に記録している第１のコンテンツ鍵、もしくは第２のコンテンツ鍵を、前記第２の装置の鍵記録部に記録し、前記第１の装置のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記第２の装置のコンテンツ記録部に記録することを特徴とする。

【００２６】

また、前記第１の装置の鍵制御部は、前記第１の装置の鍵記録部に記録している第１のコンテンツ鍵、並びに、第２のコンテンツ鍵を利用不可能な状態にして、前記第１の装置の鍵記録部に記録している第１のコンテンツ鍵、もしくは第２のコンテンツ鍵を、前記第２の装置の鍵記録部に記録し、前記第２の装置の鍵記録部に記録した第１のコンテンツ鍵

、もしくは、第２のコンテンツ鍵を、前記第１の装置の鍵記録部から消去することを特徴とする。

【００２７】

また、前記第１の暗号化コンテンツ、もしくは、前記第２の暗号化コンテンツを、前記第２の装置から前記第１の装置に移動する際、前記第１の装置の鍵制御部による制御の下で、前記第２の装置の鍵記録部に記録している第１のコンテンツ鍵、もしくは第２のコンテンツ鍵を、前記第１の装置の鍵記録部に記録し、前記第２の装置のコンテンツ記録部に記録している第１の暗号化コンテンツ、もしくは、第２の暗号化コンテンツを、前記第１の装置のコンテンツ記録部に記録することを特徴とする。

【００２８】

また、前記第１の装置の鍵制御部は、前記第１の装置の鍵記録部へ記録する第１のコンテンツ鍵、もしくは、第２のコンテンツ鍵を利用不可能な状態にして、前記第２の装置の鍵記録部に記録している第１のコンテンツ鍵、もしくは、第２のコンテンツ鍵を、前記第１の装置の鍵記録部に記録し、前記第２の装置の鍵記録部に記録している第１のコンテンツ鍵、もしくは第２のコンテンツ鍵を消去し、前記第１の装置の鍵記録部へ記録する第１のコンテンツ鍵、もしくは第２のコンテンツ鍵を利用可能な状態にすることを特徴とする。

【発明の効果】

【００２９】

本発明によれば、移動処理の実行により、オリジナルの高画質コンテンツが失われることがなく、また、移動処理時に、コンテンツの圧縮変換処理や暗号化処理が不要なため、高速に移動処理が行えるという効果を有する。

【発明を実施するための最良の形態】

【００３０】

以下、本発明の実施の形態について、図面を参照しながら説明する。図１は、本発明に係る著作権保護システムの全体構成を示すブロック図である。このシステムは、コンテンツを供給するコンテンツ供給装置１０１と、前記コンテンツを獲得して、コンテンツの記録、並びに再生を行い、さらにコンテンツの移動を実行する記録再生装置１０２と、前記移動するコンテンツを獲得する記録再生装置１０３、あるいは可搬媒体１０４からなる。

【００３１】

記録再生装置１０２は、コンテンツ供給装置１０１からコンテンツを受信して記録する際、当該コンテンツを暗号化して、例えば内蔵ＨＤＤに記録する。そして、当該コンテンツを移動する際は、移動先となる装置、あるいは可搬媒体が正規装置、あるいは正規可搬媒体であるか否かを確認（認証）した上で、コンテンツの移動を実行する。さらに、記録再生装置１０２は、コンテンツの移動が完了した後に、内部に記録するコンテンツを利用できない状態にする。ここで、認証技術は、例えば、相手が装置であれば、ＤＴＣＰ規格で定められた手順を用いることができ、相手が可搬媒体であればＣＰＲＭ　ＳＤ（Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　ｆｏｒ　Ｒｅｃｏｒｄａｂｌｅ　Ｍｅｄｉａ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ　ＳＤ　Ｍｅｍｏｒｙ　Ｃａｒｄ　Ｂｏｏｋ）規格で定められた手順を用いることができる。あるいは、非特許文献１、並びに非特許文献２に開示される公知の任意の技術を用いることができる。このように認証技術は、公知の技術で実現可能なため、その詳細についてはここでは言及しない。

【００３２】

（実施の形態１）

図２は、本発明の実施の形態１における、記録再生装置１０２がコンテンツを記録、並びに再生を行い、さらに記録再生装置１０２から可搬媒体１０４にコンテンツを移動させる場合の記録再生装置１０２、並びに可搬媒体１０４の機能を示す機能ブロック図である。

【００３３】

記録再生装置１０２は、外部からコピー制御情報と、コンテンツを受信する受信部２０

１と、前記コピー制御情報に基づき、前記受信したコンテンツを記録再生装置１０２（具体的には、後述する暗号化コンテンツ記録部２１０、２１１）に記録することが認められているか否かを判定する判定部２０２と、前記コピー制御情報を、必要に応じて更新した後、記録するコピー制御情報記録部２０４と、前記受信したコンテンツを暗号化するために用いるコンテンツ鍵を生成する鍵生成部２０５と、前記生成したコンテンツ鍵を記録するコンテンツ鍵記録部２０６と、コンテンツ鍵記録部２０６に記録したコンテンツ鍵へのアクセスを制御する制御部２０３と、前記コンテンツ鍵を用いて、前記受信したコンテンツを暗号化して、第１暗号化コンテンツを生成する暗号化部２０８と、前記第１暗号化コンテンツを記録する暗号化コンテンツ記録部２１０と、前記受信したコンテンツを、変換する変換部２０７と、前記コンテンツ鍵を用いて、前記変換したコンテンツを暗号化して第２暗号化コンテンツを生成する暗号化部２０９と、前記第２暗号化コンテンツを記録する暗号化コンテンツ記録部２１１とを備える。

【００３４】

また、記録再生装置１０２は、さらに、前記第１暗号化コンテンツ、もしくは、第２暗号化コンテンツを、前記コンテンツ鍵を用いて復号化する復号化部２２１と、復号した第１暗号化コンテンツ、もしくは、復号した第２暗号化コンテンツを再生する再生部２２２と、コピー制御情報記録部２０４に記録したコピー制御情報に基づいて、暗号化コンテンツ記録部２１１に記録した第２暗号化コンテンツを、記録再生装置１０２から可搬媒体１０４に移動することが認められているか否か判定する、もしくは、後述する可搬媒体１０４のコピー制御情報記録部２１６に記録したコピー制御情報に基づいて、可搬媒体１０４の暗号化コンテンツ記録部２１８に記録した第２暗号化コンテンツを、可搬媒体１０４から記録再生装置１０２に移動することが認められているか否か判定する判定部２１２と記録再生装置１０２と可搬媒体１０４との間で、相互に、相手が正当であるか否かを認証する認証部２２３、認証が成功した時に、記録再生装置１０２と可搬媒体１０４との間で、やり取りされるコンテンツ鍵、及び、コピー制御情報を暗号化、復号化するための暗号化／復号化部２２５、コピー制御情報記録部２０４に記録したコピー制御情報、コンテンツ鍵記録部２０６に記録したコンテンツ鍵、並びに、暗号化コンテンツ記録部２１１に記録した第２暗号化コンテンツを可搬媒体１０４に書き込む、もしくは、可搬媒体１０４から読み出す書込／読出部２１３とを備える。

【００３５】

記録再生装置１０２が備える制御部２０３、コピー制御情報記録部２０４、並びに、コンテンツ鍵記録部２０６は、外部からのデータの読み書きが不可能なセキュアな領域２１４に設けられる。この領域２１４は、具体的には、耐タンパハードウエア、耐タンパソフトウエア、あるいは、両者の組み合わせで構成する。暗号化コンテンツ記録部２１０、２１１は、外部からの読み書きが可能な領域２１５に設けられる。この領域２１５は、例えば、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）により構成する。

【００３６】

一方、可搬媒体１０４は、記録再生装置１０２と可搬媒体１０４との間で、相互に、相手が正当であるか否かを認証する認証部２２４と、認証が成功した時に、記録再生装置１０２と可搬媒体１０４との間で、やり取りされるコンテンツ鍵、及び、コピー制御情報を暗号化、復号化するための暗号化／復号化部２２６とを備える。

【００３７】

また、可搬媒体１０４は、さらに、前記第２暗号化コンテンツを記録する暗号化コンテンツ記録部２１８と、前記コンテンツ鍵を記録するコンテンツ鍵記録部２１７と、前記コピー制御情報を記録するコピー制御情報記録部２１６を備える。可搬媒体１０４が備えるコピー制御情報記録部２１６、並びに、コンテンツ鍵記録部２１７は、外部から正当な装置以外読み書きできない領域２１９に設けられる。この領域２１９は、可搬媒体１０４の認証部２２４と、記録再生装置１０２の認証部２２３との間で、認証処理が正しく実行できた場合のみ、記録再生装置１０２からのデータの読み書きが可能となる領域である。暗号化コンテンツ記録部２１８は、外部からの読み書きが可能な領域２２０に設けられる。

【００３８】
次に、図３を用いて、受信したコンテンツを記録再生装置１０２に記録する場合の動作について説明する。
【００３９】
Ｓ３０１：記録再生装置１０２の受信部２０１は、コンテンツとコピー制御情報を受信する。
【００４０】
Ｓ３０２：判定部２０２は、「前記コピー制御情報が、受信したコンテンツを記録再生装置１０２に記録することが認められているか否か」を判定する。判定の結果、「記録は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「記録は認められる」と判定した場合は、以降の処理を実行する。
【００４１】
Ｓ３０３：前記コピー制御情報を、必要に応じて更新してコピー制御情報記録部２０４に記録する。
【００４２】
Ｓ３０４：鍵生成部２０５は、コンテンツ鍵を生成し、コンテンツ鍵記録部２０６に記録する。
【００４３】
Ｓ３０５：暗号化部２０８は、受信したコンテンツを、コンテンツ鍵記録部２０６に記録しているコンテンツ鍵で暗号化して第１暗号化コンテンツを生成する。
【００４４】
Ｓ３０６：前記第１暗号化コンテンツを暗号化コンテンツ記録部２１０に記録する。
【００４５】
Ｓ３０７：変換部２０７は、受信したコンテンツを、変換する。
【００４６】
Ｓ３０８：暗号化部２０９は、前記変換したコンテンツを、コンテンツ鍵記録部２０６に記録しているコンテンツ鍵で暗号化して第２暗号化コンテンツを生成する。
【００４７】
Ｓ３０９：前記第２暗号化コンテンツを暗号化コンテンツ記録部２１１に記録する。
【００４８】
ここで、コピー制御情報としては、例えば、コピーが禁止されていることを示す「Ｃｏｐｙ　Ｎｅｖｅｒ」や、コピーが１回だけ許されていることを示す「Ｃｏｐｙ　Ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」などが用いられる。この場合、判定部２０２は、コピー制御情報が「Ｃｏｐｙ　Ｎｅｖｅｒ」であれば、「記録は認められない」と判定し、コピー制御情報が「Ｃｏｐｙ　Ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」であれば、「記録は認められている」と判定する。後者の場合、コンテンツを記録再生装置に記録するのに伴い、コピー制御情報は、「Ｃｏｐｙ　Ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」から、コピー禁止を示す「Ｎｏ　Ｍｏｒｅ　Ｃｏｐｙ」へ更新してコピー制御情報記録部２０４に記録する。
【００４９】
変換部２０７は、例えば、受信したコンテンツが、ＭＰＥＧ２形式の映像コンテンツである場合に、ＭＰＥＧ４形式の映像コンテンツに変換する。
【００５０】
次に、図４を用いて、記録再生装置１０２から、可搬媒体１０４へコンテンツを移動する場合の動作について説明する。
【００５１】
Ｓ４０１：記録再生装置１０２の判定部２１２は、書込／読出部２１３を介して、コピー制御情報記録部２０４に記録されているコピー制御情報を受け取り、「受け取ったコピー制御情報が、暗号化コンテンツ記録部２１１に記録した第２暗号化コンテンツを可搬媒体１０４に移動することが認められているか否か」を判定する。判定の結果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認

められる」と判定した場合は、以降の処理を実行する。

【００５２】

Ｓ４０２：記録再生装置１０４の認証部２２３は、可搬媒体１０４の認証部２２４との間で相互認証を行い、相互認証が成功した時は、認証部２２３、２２４はそれぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

【００５３】

Ｓ４０３：書込／読出部２１３は、コピー制御情報記録部２０４に記録しているコピー制御情報、並びに、コンテンツ鍵記録部２０６に記録しているコンテンツ鍵を読み出す。

【００５４】

このとき、制御部２０３は、コンテンツ鍵記録部２０６に記録しているコンテンツ鍵が、以降、アクセスできないように利用不可状態にする。

【００５５】

Ｓ４０４：書込／読出部２１３は、読み出したコピー制御情報、並びに、コンテンツ鍵を、暗号化／復号化部２２５にて、前記セッション鍵を用いて暗号化して可搬媒体１０４に送り、可搬媒体１０４は、受け取った暗号化したコピー制御情報、並びに、コンテンツ鍵を、暗号化／復号化部２２６にて、前記セッション鍵を用いて復号し、復号したコピー制御情報、並びに、コンテンツ鍵を可搬媒体１０４に記録する。

【００５６】

Ｓ４０５：コピー制御情報記録部２０４に記録しているコピー制御情報と、コンテンツ鍵記録部２０６に記録しているコンテンツ鍵を消去する。

【００５７】

Ｓ４０６：書込／読出部２１３は、暗号化コンテンツ記録部２１１に記録している第２暗号化コンテンツを読出す。

【００５８】

Ｓ４０７：読み出した第２暗号化コンテンツを可搬媒体１０４に記録する。

【００５９】

Ｓ４０８：暗号化コンテンツ記録部２１１に記録している第２暗号化コンテンツを消去する。

【００６０】

図５、図６は、上記動作における記録再生装置１０２、並びに可搬媒体１０４における各データの記録状態を示した図である。図５（ａ）は、上記ステップＳ４０１の開始時点、（ｂ）は、上記ステップＳ４０３の終了時点、（ｃ）は、ステップＳ４０４の終了時点、（ｄ）は、ステップＳ４０５の終了時点、図６（ｅ）は、ステップＳ４０７の終了時点、（ｆ）は、ステップＳ４０８の終了時点である。

【００６１】

ここで、ステップＳ４０３において、制御部２０３は、コンテンツ鍵記録部２０６に記録しているコンテンツ鍵が、以降、アクセスできないよう利用不可状態にする。これにより、ステップＳ４０４が終了し、ステップＳ４０５が開始する前のタイミングで（図５（ｃ））、電源断、もしくは、可搬媒体１０４を記録再生装置１０２から不正に引き抜く事などが行われたとしても、記録再生装置１０２と、可搬媒体１０４の両方において同時にコンテンツ鍵が利用可能な状態で存在することを防止できる。また、図５（ａ）～図６（ｆ）のどのタイミングで電源断が起こっても、記録再生装置１０２と、可搬媒体１０４のいずれかにおいてコンテンツ鍵は存在するため、移動元と移動先の両方でコンテンツ鍵が共に損なわれコンテンツが利用できなくなることはない。

【００６２】

ステップＳ４０２における認証部２２３、２２４で実行される相互認証、及び、セッション鍵共有方法としては、例えば、チャレンジーレスポンス型の相互認証、セッション鍵共有方法を用いる。チャレンジーレスポンス型の相互認証、セッション鍵共有方法については、公知であるので説明は省略する。

【００６３】

次に、図７を用いて、可搬媒体１０４から、記録再生装置１０２へコンテンツを移動する場合の動作について説明する。

【００６４】

Ｓ６０１：記録再生装置１０２の判定部２１２は、書込／読出部２１３を介して、可搬媒体１０４のコピー制御情報記録部２１６に記録されているコピー制御情報を受け取り、「受け取ったコピー制御情報が、可搬媒体１０４の暗号化コンテンツ記録部２１８に記録した第２暗号化コンテンツを記録再生装置１０２に移動することが認められているか否か」を判定する。判定の結果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認められる」と判定した場合は、以降の処理を実行する。

【００６５】

Ｓ６０２：記録再生装置１０４の認証部２２３は、可搬媒体１０４の認証部２２４との間で相互認証を行い、相互認証が成功した時は、認証部２２３、２２４はそれぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

【００６６】

Ｓ６０３：書込／読出部２１３は、可搬媒体１０４のコピー制御情報記録部２１６に記録しているコピー制御情報、並びに、コンテンツ鍵記録部２１７に記録しているコンテンツ鍵を読み出す。このとき、可搬媒体１０４の暗号化／復号化部２２６にて、コピー制御情報、並びに、コンテンツ鍵は、前記セッション鍵を用いて暗号化して、記録再生装置１０２に送り、記録再生装置１０２の暗号化／復号化部２２５は、受け取った暗号化したコピー制御情報、並びに、コンテンツ鍵を、前記セッション鍵を用いて復号して、書込／読出部２１３に送る。

【００６７】

Ｓ６０４：書込／読出部２１３は、読み出したコピー制御情報、並びに、コンテンツ鍵を、記録再生装置１０２のコピー制御情報記録部２０４、並びに、コンテンツ鍵記録部２０６にそれぞれ記録する。このとき、制御部２２３は、コンテンツ鍵記録部２０６に記録したコンテンツ鍵はアクセスできないよう利用不可状態にする。

【００６８】

Ｓ６０５：可搬媒体１０４のコピー制御情報記録部２１６に記録しているコピー制御情報、並びに、コンテンツ鍵記録部２１７に記録しているコンテンツ鍵を消去する。

【００６９】

制御部２２３は、コンテンツ鍵記録部２０６に記録したコンテンツ鍵がアクセスできるように利用可能状態にする。

【００７０】

Ｓ６０６：書込／読出部２１３は、可搬媒体１０４の暗号化コンテンツ記録部２１８に記録している第２暗号化コンテンツを読出す。

【００７１】

Ｓ６０７：読み出した第２暗号化コンテンツを記録再生装置１０２の暗号化コンテンツ記録部２１１に記録する。

【００７２】

Ｓ６０８：可搬媒体１０４の暗号化コンテンツ記録部２１８に記録している第２暗号化コンテンツを消去する。

【００７３】

図８、図９は、上記動作における記録再生装置１０２、並びに可搬媒体１０４における各データの記録状態を示した図である。図８（ａ）は、上記ステップＳ６０１の開始時点、（ｂ）は、上記ステップＳ６０４の終了時点、（ｃ）は、ステップＳ６０５の終了時点、（ｄ）は、ステップＳ６０７の終了時点、図９（ｅ）は、ステップＳ６０８の終了時点である。

【００７４】

次に、図１０を用いて、記録再生装置１０２において、記録した第１暗号化コンテンツ

、もしくは、第２暗号化コンテンツを再生する場合の動作について説明する。

【００７５】

Ｓ８０１：復号化部２２１は、暗号化コンテンツ記録部２１０、もしくは、暗号化コンテンツ記録部２１１より、第１暗号化コンテンツ、もしくは、第２暗号化コンテンツを読出す。

【００７６】

Ｓ８０２：復号化部２２１は、コンテンツ鍵記録部２０６より、コンテンツ鍵を読み出す。

【００７７】

このとき、制御部２０３は、コンテンツ鍵記録部２０６に記録しているコンテンツ鍵が、以降、アクセスできないよう利用不可状態にする。

【００７８】

Ｓ８０３：復号化部２２１は、読み出した第１暗号化コンテンツ、もしくは、第２暗号化コンテンツを、読み出したコンテンツ鍵を用いて復号化する。

【００７９】

Ｓ８０４：再生部２２２は、復号した第１暗号化コンテンツもしくは、第２暗号化コンテンツを再生する。再生が終了すると、コンテンツ鍵記録部２０６に記録しているコンテンツ鍵を利用可能状態にする。

【００８０】

ここで、ステップＳ８０２において、制御部２０３により、コンテンツ鍵はアクセスできない利用不可状態にされるので、第１暗号化コンテンツの復号及び再生処理と、第２暗号化コンテンツの復号及び再生処理は、排他的にしか実行できない。

【００８１】

（変形例）

実施の形態１では、第２暗号化コンテンツが記録再生装置１０２から可搬媒体１０４に移動する場合において、記録再生装置１０２の制御部２０３が、コンテンツ鍵が読み出されたときアクセスできないように利用不可状態にしたが、この構成に変えて、可搬媒体１０４の領域２１９に制御部を設けても良い。この場合、第２暗号化コンテンツが記録再生装置１０２から可搬媒体１０４に移動する場合の動作は次の通りである。

【００８２】

Ｔ４０１：記録再生装置１０２の判定部２１２は、書込／読出部２１３を介して、コピー制御情報記録部２０４に記録されているコピー制御情報を受け取り、「受け取ったコピー制御情報が、暗号化コンテンツ記録部２１１に記録した第２暗号化コンテンツを可搬媒体１０４に移動することが認められているか否か」を判定する。判定の結果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認められる」と判定した場合は、以降の処理を実行する。

【００８３】

Ｔ４０２：記録再生装置１０４の認証部２２３は、可搬媒体１０４の認証部２２４との間で相互認証を行い、相互認証が成功した時は、認証部２２３、２２４はそれぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

【００８４】

Ｔ４０３：書込／読出部２１３は、コピー制御情報記録部２０４に記録しているコピー制御情報、並びに、コンテンツ鍵記録部２０６に記録しているコンテンツ鍵を読み出す。

【００８５】

Ｔ４０４：書込／読出部２１３は、読み出したコピー制御情報、並びに、コンテンツ鍵を、暗号化／復号化部２２５にて、前記セッション鍵を用いて暗号化して可搬媒体１０４に送り、可搬媒体１０４は、受け取った暗号化したコピー制御情報、並びに、コンテンツ鍵を、暗号化／復号化部２２６にて、前記セッション鍵を用いて復号し、復号したコピー制御情報、並びに、コンテンツ鍵を可搬媒体１０４に記録する。

【００８６】

このとき、可搬媒体の制御部は、可搬媒体１０４のコンテンツ鍵記録部２１７に記録しているコンテンツ鍵が、アクセスできないように利用不可状態にする。

【００８７】

Ｔ４０５：コピー制御情報記録部２０４に記録しているコピー制御情報、並びに、コンテンツ鍵記録部２０６に記録しているコンテンツ鍵を消去する。

【００８８】

このとき、可搬媒体１０４の制御部は、コンテンツ鍵記録部２１７に記録しているコンテンツ鍵が、アクセスできるように利用可能状態にする。

【００８９】

Ｔ４０６：書込／読出部２１３は、暗号化コンテンツ記録部２１１に記録している第２暗号化コンテンツを読出す。

【００９０】

Ｔ４０７：読み出した第２暗号化コンテンツを可搬媒体１０４に記録する。

【００９１】

Ｔ４０８：暗号化コンテンツ記録部２１１に記録している第２暗号化コンテンツを消去する。

【００９２】

同様に、実施の形態１では、第２暗号化コンテンツが可搬媒体１０４から記録再生装置１０２に移動する場合において、記録再生装置１０２の制御部２０３が、コンテンツ鍵が読み出されたときアクセスできないように利用不可状態にしたが、この構成に変えて、可搬媒体１０４の領域２１９に制御部を設けても良い。この場合の動作については、上記ステップＴ４０１からＴ４０８と同様であるので説明は省略する。

【００９３】

また、実施の形態１では、記録再生装置１０２に制御部２０３を設ける構成としたが、記録再生装置１０２と、可搬媒体１０４の双方に、制御部を設ける構成としてもよい。

【００９４】

以上、本発明の実施の形態１では、受信したコンテンツと、それを変換したコンテンツとを、それぞれ、同一のコンテンツ鍵を用いて、暗号化する構成について説明したが、この構成に限定されない。すなわち、受信したコンテンツと、それを変換したコンテンツとを、異なるコンテンツ鍵を用いて、暗号化する構成としてもよい。この場合について、以下、実施の形態２として説明する。

【００９５】

（実施の形態２）

図１１は、本発明の実施の形態２における、記録再生装置１０２ａがコンテンツを記録、並びに再生を行い、さらに記録再生装置１０２ａから可搬媒体１０４ａにコンテンツを移動させる場合の記録再生装置１０２ａ、並びに可搬媒体１０４ａの機能を示す機能ブロック図である。

【００９６】

記録再生装置１０２ａは、外部からコピー制御情報と、コンテンツを受信する受信部２０１ａと、前記コピー制御情報に基づき、前記受信したコンテンツを記録再生装置１０２ａ（具体的には、後述する暗号化コンテンツ記録部２１０ａ、２１１ａ）に記録することが認められているか否かを判定する判定部２０２ａと、前記コピー制御情報を、必要に応じて更新した後、記録するコピー制御情報記録部２０４ａと、前記受信したコンテンツを暗号化するために用いる第１コンテンツ鍵と、第２コンテンツ鍵を生成する鍵生成部２０５ａと、前記生成した第１コンテンツ鍵を記録するコンテンツ鍵記録部２０６ａ１と、前記生成した第２コンテンツ鍵を記録するコンテンツ鍵記録部２０６ａ２と、コンテンツ鍵記録部２０６ａ１、２０６ａ２に記録された第１コンテンツ鍵、第２コンテンツ鍵へのアクセスを制御する制御部２０３ａと、前記第１コンテンツ鍵を用いて、前記受信したコンテンツを暗号化して、第１暗号化コンテンツを生成する暗号化部２０８ａと、前記第１暗号化コンテンツを記録する暗号化コンテンツ記録部２１０ａと、前記受信したコンテンツ

を、変換する変換部２０７ａと、前記第２コンテンツ鍵を用いて、前記変換したコンテンツを暗号化して第２暗号化コンテンツを生成する暗号化部２０９ａとを備える。

【００９７】

また、記録再生装置１０２ａは、さらに、前記第２暗号化コンテンツを記録する暗号化コンテンツ記録部２１１ａと、前記第１暗号化コンテンツ、もしくは、第２暗号化コンテンツを、前記第１コンテンツ鍵、もしくは、前記第２コンテンツ鍵を用いて復号化する復号化部２２１ａと、復号した第１暗号化コンテンツ、もしくは、復号した第２暗号化コンテンツを再生する再生部２２２ａと、コピー制御情報記録部２０４ａに記録したコピー制御情報に基づいて、暗号化コンテンツ記録部２１１ａに記録した第２暗号化コンテンツを、記録再生装置１０２ａから可搬媒体１０４ａに移動することが認められているか否か判定する、もしくは、後述する可搬媒体１０４ａのコピー制御情報記録部２１６ａに記録したコピー制御情報に基づいて、可搬媒体１０４ａの暗号化コンテンツ記録部２１８ａに記録した第２暗号化コンテンツを、可搬媒体１０４ａから記録再生装置１０２ａに移動することが認められているか否か判定する判定部２１２ａと、記録再生装置１０２ａと可搬媒体１０４ａとの間で、相互に、相手が正当であるか否かを認証する認証部２２３ａ、認証部２２４ａと、認証が成功した時に、記録再生装置１０２ａと可搬媒体１０４ａとの間で、やりとりされるコピー制御情報、並びに、第１コンテンツ鍵、もしくは、第２コンテンツ鍵を暗号化、復号化するための暗号化／復号化部２２５ａ、２２６ａと、コピー制御情報記録部２０４ａに記録したコピー制御情報と、コンテンツ鍵記録部２０６ａ１に記録した第１コンテンツ鍵、もしくは、コンテンツ鍵記録部２０６ａ２に記録した第２コンテンツ鍵と、並びに、暗号化コンテンツ記録部２１１ａに記録した第２暗号化コンテンツを可搬媒体１０４ａに書込む、もしくは、可搬媒体１０４ａから読み出す書込／読出部２１３ａとを備える。

【００９８】

記録再生装置が備えるコピー制御情報記録部２０４ａ、制御部２０３ａ、並びに、コンテンツ鍵記録部２０６ａ１、２０６ａ２は、外部からのデータの読み書きが不可能なセキュアな領域２１４ａに設けられる。この領域２１４ａは、具体的には、耐タンパハードウエア、耐タンパソフトウエア、あるいは、両者の組み合わせで構成する。暗号化コンテンツ記録部２１０ａ、２１１ａは、外部からの読み書きが可能な領域２１５ａに設けられる。この領域２１５ａは、例えば、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）により構成する。

【００９９】

一方、可搬媒体１０４ａは、記録再生装置１０２ａと可搬媒体１０４ａとの間で、相互に、相手が正当であるか否かを認証する認証部２２４ａと、認証が成功した時に、記録再生装置１０２ａと可搬媒体１０４ａとの間で、やりとりされるコピー制御情報、並びに、第１コンテンツ鍵、もしくは、第２コンテンツ鍵を暗号化、復号化するための暗号化／復号化部２２６ａとを備える。

【０１００】

また、可搬媒体１０４ａは、さらに、前記第２暗号化コンテンツを記録する暗号化コンテンツ記録部２１８ａと、前記第１コンテンツ鍵、もしくは、第２コンテンツ鍵を記録するコンテンツ鍵記録部２１７ａと、前記コピー制御情報を記録するコピー制御情報記録部２１６ａを備える。可搬媒体１０４ａが備えるコピー制御情報記録部２１６ａ、並びに、前記コンテンツ鍵記録部２１７ａは、外部から正当な装置以外読み書きできない領域２１９ａに設けられる。この領域２１９ａは、可搬媒体１０４ａの認証部２２４ａと、記録再生装置の認証部２２３ａとの間で、認証処理が正しく実行できた場合のみ、前記記録再生装置１０２ａからのデータの読み書き可能となる領域である。暗号化コンテンツ記録部２１８ａは、外部からの読み書きが可能な領域２２０ａに設けられる。

【０１０１】

次に、図１２を用いて、受信したコンテンツを記録再生装置１０２ａに記録する場合の動作について説明する。

【０１０２】
Ｓ３０１ａ：記録再生装置１０２ａの受信部２０１ａは、コンテンツとコピー制御情報を受信する。
【０１０３】
Ｓ３０２ａ：判定部２０２ａは、「前記コピー制御情報が、受信したコンテンツを記録再生装置１０２ａに記録することが認められているか否か」を判定する。判定の結果、「記録は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「記録は認められる」と判定した場合は、以降の処理を実行する。
【０１０４】
Ｓ３０３ａ：前記コピー制御情報を、必要に応じて更新してコピー制御情報記録部２０４ａに記録する。
【０１０５】
Ｓ３０４ａ：鍵生成部２０５ａは、第１コンテンツ鍵、および、第２コンテンツ鍵を生成し、それぞれコンテンツ鍵記録部２０６ａ１、２０６ａ２に記録する。
【０１０６】
Ｓ３０５ａ：暗号化部２０８ａは、受信したコンテンツを、コンテンツ鍵記録部２０６ａ１に記録している第１コンテンツ鍵で暗号化して第１暗号化コンテンツを生成する。
【０１０７】
Ｓ３０６ａ：前記第１暗号化コンテンツを暗号化コンテンツ記録部２１０ａに記録する。
【０１０８】
Ｓ３０７ａ：変換部２０７ａは、受信したコンテンツを、変換する。
【０１０９】
Ｓ３０８ａ：暗号化部２０９ａは、前記変換したコンテンツを、コンテンツ鍵記録部２０６ａ２に記録している第２コンテンツ鍵で暗号化して第２暗号化コンテンツを生成する。
【０１１０】
Ｓ３０９ａ：前記第２暗号化コンテンツを暗号化コンテンツ記録部２１１ａに記録する。
【０１１１】
ここで、コピー制御情報としては、実施の形態１の場合と同様に、例えば、コピーが禁止されていることを示す「Ｃｏｐｙ　Ｎｅｖｅｒ」や、コピーが１回だけ許されていることを示す「Ｃｏｐｙ　Ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」などが用いられる。この場合、判定部２０２ａは、コピー制御情報が「Ｃｏｐｙ　Ｎｅｖｅｒ」であれば、「記録は認められない」と判定し、コピー制御情報が「Ｃｏｐｙ　Ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」であれば、「記録は認められている」と判定する。後者の場合、コンテンツを記録再生装置に記録するのに伴い、コピー制御情報は、「Ｃｏｐｙ　Ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」から、これ以上コピー禁止を示す「Ｎｏ　Ｍｏｒｅ　Ｃｏｐｙ」へ更新してコピー制御情報記録部２０４ａに記録する。
【０１１２】
変換部２０７ａは、例えば、受信したコンテンツが、ＭＰＥＧ２形式の映像コンテンツである場合に、ＭＰＥＧ４形式の映像コンテンツに圧縮変換する。
【０１１３】
次に、図１３を用いて、記録再生装置１０２ａから、可搬媒体１０４ａへコンテンツを移動する場合の動作について説明する。
【０１１４】
Ｓ４０１ａ：記録再生装置１０２ａの判定部２１２ａは、書込／読出部２１３ａを介して、コピー制御情報記録部２０４ａに記録されているコピー制御情報を受け取り、「受け取ったコピー制御情報が、暗号化コンテンツ記録部２１１ａに記録した第２暗号化コンテンツを可搬媒体１０４ａに移動することが認められているか否か」を判定する。判定の結

果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認められる」と判定した場合は、以降の処理を実行する。

【０１１５】

Ｓ４０２ａ：記録再生装置１０４ａの認証部２２３ａは、可搬媒体１０４ａの認証部２２４ａとの間で相互認証を行い、相互認証が成功した時は、認証部２２３ａ、２２４ａはそれぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

【０１１６】

Ｓ４０３ａ：書込／読出部２１３ａは、コピー制御情報記録部２０４ａに記録しているコピー制御情報、並びに、コンテンツ鍵記録部２０６ａ２に記録している第２コンテンツ鍵を読み出す。

【０１１７】

このとき、制御部２０３ａは、コンテンツ鍵記録部２０６ａ１に記録している第１コンテンツ鍵および、コンテンツ鍵記録部２０６ａ２に記録している第２コンテンツ鍵が、以降、アクセスできないように利用不可状態にする。

【０１１８】

Ｓ４０４ａ：書込／読出部２１３は、読み出したコピー制御情報、並びに、第２コンテンツ鍵を、暗号化／復号化部２２５ａにて、前記セッション鍵を用いて暗号化して可搬媒体１０４ａに送り、可搬媒体１０４ａは、受け取った暗号化したコピー制御情報、並びに、第２コンテンツ鍵を、暗号化／復号化部２２６ａにて、前記セッション鍵を用いて復号し、復号したコピー制御情報、並びに、第２コンテンツ鍵を可搬媒体１０４ａに記録する。

【０１１９】

Ｓ４０５ａ：コピー制御情報記録部２０４ａに記録しているコピー制御情報、並びに、コンテンツ鍵記録部２０６ａ２に記録している第２コンテンツ鍵を消去する。

【０１２０】

Ｓ４０６ａ：書込／読出部２１３ａは、暗号化コンテンツ記録部２１１ａに記録している第２暗号化コンテンツを読出す。

【０１２１】

Ｓ４０７ａ：読み出した第２暗号化コンテンツを可搬媒体１０４ａに記録する。

【０１２２】

Ｓ４０８ａ：暗号化コンテンツ記録部２１１ａに記録している第２暗号化コンテンツを消去する。

【０１２３】

図１４、図１５は、上記動作における記録再生装置１０２ａ、並びに可搬媒体１０４ａにおける各データの記録状態を示した図である。図１４（ａ）は、上記ステップＳ４０１ａの開始時点、（ｂ）は、上記ステップＳ４０３ａの終了時点、（ｃ）は、ステップＳ４０４ａの終了時点、（ｄ）は、ステップＳ４０５ａの終了時点、図１５（ｅ）は、ステップＳ４０７ａの終了時点、（ｆ）は、ステップＳ４０８ａの終了時点である。

【０１２４】

ここでステップＳ４０３ａにおいて、制御部２０３ａは、コンテンツ鍵記録部２０６ａ１に記録している第１コンテンツ鍵、及び、コンテンツ鍵記録部２０６ａ２に記録している第２コンテンツ鍵が、以降、アクセスできないよう利用不可状態にする。これにより、ステップＳ４０４ａが終了し、ステップＳ４０５ａが開始する前のタイミングで、電源断、もしくは、可搬媒体１０４ａを記録再生装置１０２ａから不正に引き抜く事などが行われたとしても、記録再生装置１０２ａと、可搬媒体１０４ａの両方において同時に、第１コンテンツ鍵と第２コンテンツ鍵が利用可能な状態で存在することを防止できる。また、図１４（ａ）～図１５（ｆ）のどのタイミングで電源断が起こっても、記録再生装置１０２ａと、可搬媒体１０４ａのいずれかにおいて第１コンテンツ鍵、及び、第２コンテンツ鍵は存在するため、移動元と移動先の両方で、第１コンテンツ鍵、及び、第２コンテンツ

鍵が共に損なわれコンテンツが利用できなくなることはない。

【０１２５】

ステップＳ４０２ａにおける認証部２２３ａ、２２４ａで実行される相互認証、及び、セッション鍵共有方法としては、実施の形態１と同様に、例えば、チャレンジーレスポンス型の相互認証、セッション鍵共有方法を用いる。チャレンジーレスポンス型の相互認証、セッション鍵共有方法については、公知であるので説明は省略する。

【０１２６】

次に、図１６を用いて、可搬媒体１０４ａから、記録再生装置１０２ａへコンテンツを移動する場合の動作について説明する。

【０１２７】

Ｓ６０１ａ：記録再生装置１０２ａの判定部２１２ａは、書込／読出部２１３ａを介して、可搬媒体１０４ａのコピー制御情報記録部２１６ａに記録されているコピー制御情報を受け取り、「受け取ったコピー制御情報が、可搬媒体１０４ａの暗号化コンテンツ記録部２１８ａに記録した第２暗号化コンテンツを記録再生装置１０２ａに移動することが認められているか否か」を判定する。判定の結果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認められる」と判定した場合は、以降の処理を実行する。

【０１２８】

Ｓ６０２ａ：記録再生装置１０４ａの認証部２２３ａは、可搬媒体１０４ａの認証部２２４ａとの間で相互認証を行い、相互認証が成功した時は、認証部２２３ａ、２２４ａはそれぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

【０１２９】

Ｓ６０３ａ：書込／読出部２１３ａは、可搬媒体１０４ａのコピー制御情報記録部２１６ａに記録しているコピー制御情報、並びに、コンテンツ鍵記録部２１７ａに記録している第２コンテンツ鍵を読み出す。このとき、可搬媒体１０４ａの暗号化／復号化部２２６ａにて、コピー制御情報、並びに、第２コンテンツ鍵は、前記セッション鍵を用いて暗号化して、記録再生装置１０２ａに送り、記録再生装置１０２ａの暗号化／復号化部２２５ａは、受け取った暗号化したコピー制御情報、並びに、第２コンテンツ鍵を、前記セッション鍵を用いて復号して、書込／読出部２１３ａに送る。

【０１３０】

Ｓ６０４ａ：書込／読出部２１３ａは、読み出したコピー制御情報、並びに、第２コンテンツ鍵を、記録再生装置１０２ａのコピー制御情報記録部２０４ａ、並びに、コンテンツ鍵記録部２０６ａ２にそれぞれ記録する。このとき、制御部２０３ａは、コンテンツ鍵記録部２０６ａ２に記録した第２コンテンツ鍵はアクセスできないよう利用不可状態にする。

【０１３１】

Ｓ６０５ａ：可搬媒体１０４ａのコピー制御情報記録部２１６ａに記録しているコピー制御情報、並びに、コンテンツ鍵記録部２１７ａに記録している第２コンテンツ鍵を消去する。

【０１３２】

制御部２０３ａは、コンテンツ鍵記録部２０６ａ２に記録したコンテンツ鍵、並びに、コンテンツ鍵記録部２０６ａ１に記録した第１コンテンツ鍵を利用可能状態にする。

【０１３３】

Ｓ６０６ａ：書込／読出部２１３ａは、可搬媒体１０４ａの暗号化コンテンツ記録部２１８ａに記録している第２暗号化コンテンツを読出す。

【０１３４】

Ｓ６０７ａ：読み出した第２暗号化コンテンツを記録再生装置１０２ａの暗号化コンテンツ記録部２１１ａに記録する。

【０１３５】

Ｓ６０８ａ：可搬媒体１０４ａの暗号化コンテンツ記録部２１８ａに記録している第２暗号化コンテンツを消去する。

【０１３６】

図１７、図１８は、上記動作における記録再生装置１０２ａ、並びに可搬媒体１０４ａにおける各データの記録状態を示した図である。図１７（ａ）は、上記ステップＳ６０１ａの開始時点、（ｂ）は、上記ステップＳ６０４ａの終了時点、（ｃ）は、ステップＳ６０５ａの終了時点、（ｄ）は、ステップＳ６０７ａの終了時点、図１８（ｅ）は、ステップＳ６０８ａの終了時点である。

【０１３７】

次に、図１９を用いて、記録再生装置１０２ａにおいて、記録した第１暗号化コンテンツ、もしくは、第２暗号化コンテンツを再生する場合の動作について説明する。

【０１３８】

Ｓ７０１ａ：復号化部２２１ａは、暗号化コンテンツ記録部２１０ａ、もしくは、暗号化コンテンツ記録部２１１ａより、第１暗号化コンテンツ、もしくは、第２暗号化コンテンツを読出す。

【０１３９】

Ｓ７０２ａ：復号化部２２１ａは、コンテンツ鍵記録部２０６ａ１より第１コンテンツ鍵を、もしくは、コンテンツ鍵記録部２０６ａ２より第２コンテンツ鍵を読み出す。

【０１４０】

このとき、制御部２０３ａは、コンテンツ鍵記録部２０６ａ１に記録している第１コンテンツ鍵、及び、コンテンツ鍵記録部２０６ａ２に記録している第２コンテンツ鍵が、以降、アクセスできないよう利用不可状態にする。

【０１４１】

Ｓ７０３ａ：復号化部２２１ａは、読み出した第１暗号化コンテンツ、もしくは、第２暗号化コンテンツを、読み出した第１コンテンツ鍵、もしくは、第２コンテンツ鍵を用いて復号化する。

【０１４２】

Ｓ７０４ａ：再生部２２２ａは、復号した第１暗号化コンテンツもしくは、第２暗号化コンテンツを再生する。

【０１４３】

ここで、ステップＳ７０２ａにおいて、制御部２０３ａにより、第１コンテンツ鍵、もしくは、第２コンテンツ鍵はアクセスできないよう利用不可状態にされるので、第１暗号化コンテンツの復号及び再生処理と、第２暗号化コンテンツの復号及び再生処理は、排他的にしか実行できない。

【０１４４】

（その他の変形例）

（１）上記実施の形態１、及び上記実施の形態２において、コンテンツ供給装置１０１、１０１ａから記録再生装置１０２、１０２ａへのコンテンツの供給方法としては、地上波、あるいは、衛星などを介した放送、インターネットなどを介した通信、ＤＶＤなどの記録メディアを介した方法など、さまざまな方法が利用できる。

【０１４５】

（２）上記実施の形態１、及び上記実施の形態２において、受信部２０１、２０１ａにて、受信したコンテンツや、コピー制御情報は、暗号化されていてもよい。この場合は、判定部２０２、２０２ａで処理する前に、暗号化されたコンテンツやコピー制御情報は復号化するものとする。

【０１４６】

（３）上記実施の形態１、及び上記実施の形態２では、受信したコンテンツから、１つの変換したコンテンツを作成し、暗号化して記録する構成を説明したが、この構成に限定されない。例えば、受信したコンテンツから、複数の異なる変換を施したコンテンツを作成し、暗号化して記録し、そのうちの一つないし複数を記録再生装置から可搬媒体に移動

するように構成してもよい。また実施の形態１、及び実施の形態２では、受信したコンテンツ自身は変換しない構成としたが、受信したコンテンツ自身を、（第２暗号化コンテンツとは異なる形式で）変換したものであるとしてもよい。

【０１４７】

（４）上記実施の形態１、及び上記実施の形態２では、記録再生装置１０２、１０２ａの鍵生成部２０５、２０５ａにて、コンテンツ鍵、第１コンテンツ鍵、第２コンテンツ鍵を生成し、コンテンツ鍵記録部２０６、２０６ａ１、２０６ａ２に記録するものとしたが、この構成に限定されない。例えば、コンテンツ鍵は、外部で生成され、記録再生装置１０２、１０２ａに供給される構成としてもよい。

【０１４８】

（５）上記実施の形態１、及び上記実施の形態２において、可搬媒体１０４、１０４ａとしては、例えば、ＳＤメモリカードを用いることができる。この場合、認証部２２３、２２４、２２３ａ、２２４ａ、及び、暗号化／復号化部２２５、２２６、２２５ａ、２２６ａは、ＣＰＲＭ　ＳＤ規格により決められた方式に従って実行する。

【０１４９】

（６）上記実施の形態１、及び上記実施の形態２では、第２暗号化コンテンツを、記録再生装置１０２、１０２ａから可搬媒体１０４、１０４ａに移動する場合について説明したが、第１暗号化コンテンツを記録再生装置１０２、１０２ａから可搬媒体１０４、１０４ａに移動するとしてもよい。

【０１５０】

（７）上記実施の形態１、及び上記実施の形態２では、記録再生装置から可搬媒体へコンテンツを移動する、あるいは可搬媒体から記録再生装置へコンテンツを移動する構成としたが、本発明はその構成に限定されるものではない。例えば、記録再生装置から、別の記録再生装置へコンテンツを移動する構成であってもよい。

【０１５１】

（８）このとき、例えば、記録再生装置１０２、及び、記録再生装置１０３の認証部、及び、暗号化／復号化部は、ＤＴＣＰ規格により決められた方式に従って実行する。

【０１５２】

（９）上記実施の形態１、及び上記実施の形態２では、記録再生装置から可搬媒体へコンテンツを移動する、あるいは可搬媒体から記録再生装置へコンテンツを移動する際、記録再生装置、並びに可搬媒体に記録する各種データを消去する構成としたが、本発明はその構成に限定されるものではない。例えば、可搬媒体に記録する暗号化コンテンツは消去せずに、復号に必要なコンテンツ鍵だけを消去して、前記暗号化コンテンツを利用不可状態にする構成であってもよい。また、データの消去ではなく、データの一部を破壊して利用できない状態にする構成であってもよい。また、データの消去ではなく、データを不正にアクセスできない利用不可能状態にする構成であってもよい。

【０１５３】

（１０）上記実施の形態１、及び上記実施の形態２において、記録再生装置が、コンテンツの移動処理における状態遷移を記憶する記憶部を備える構成であってもよい。記録再生装置は、コンテンツの移動が正しく完了しなかった場合、前記記憶部に記憶する状態遷移に基づいて、コンテンツの移動処理を続けて行うか、コンテンツの移動処理を最初からやり直すかを判断する構成であってもよい。さらに、記録再生装置は、前記記憶部に記憶する状態遷移を利用者に通知する通知部を備える構成であってもよい。その場合、正しく完了しなかった旨を利用者に通知して、利用者からの指示に基づいて、コンテンツの移動処理を続けるか、あるいはコンテンツの移動処理を最初かやり直すかを決定する構成であってもよい。

【０１５４】

（１１）上記実施の形態１、及び上記実施の形態２において、記録再生装置、並びに可搬媒体が、コンテンツ鍵を移動後に消去する場合、コンテンツ鍵の受信側が、コンテンツ鍵の送信側に対して正しく受信できたことを通知して、送信側は前記通知に基づいて受信

を確認した後に、コンテンツ鍵を消去する構成であってもよい。

【０１５５】

（１２）上記実施の形態１、及び上記実施の形態２において、コンテンツには当該コンテンツを一意に識別するための識別子が付与されており、可搬媒体に移動させたコンテンツを元の記録再生装置に戻す場合、前記記録再生装置は、自身が保持する暗号化コンテンツの識別子、並びに可搬媒体に記録する暗号化コンテンツの識別子が一致するか否かを判定して、一致した場合に限り、コンテンツを記録再生装置に移動させることを許可する構成であってもよい。また、コンテンツには、コンテンツを一意に識別する識別子の代わりに、移動元の記録再生装置を一意に識別する識別子が付与されている構成であってもよい。この場合、記録再生装置は、コンテンツに付与されている記録再生装置の識別子と、自身の識別子が一致するか否かを判定して、一致した場合に限り、コンテンツを記録再生装置に移動させることを許可する構成であってもよい。

【０１５６】

（１３）上記実施の形態１、及び上記実施の形態２において、複数のコンテンツに対する、第１暗号化コンテンツ、第２暗号化コンテンツをそれぞれ作成し、暗号化コンテンツ記録部２１０、２１１、２１０ａ、２１１ａに記録し、複数のコンテンツに対する、コピー制御情報、並びに、コンテンツ鍵（もしくは、第１コンテンツ鍵、第２コンテンツ鍵）を、それぞれコピー制御情報記録部２０４、２０４ａ、コンテンツ鍵記録部２０６、２０６ａ１、２０６ａ２に記録する構成としてもよい。この場合、コンテンツと、それに対応するコンテンツ鍵、並びに、コピー制御情報が分かるように、例えば、コンテンツ識別情報を、第１暗号化コンテンツ、及び、第２暗号化コンテンツを、暗号化コンテンツ記録部２１０、２１１、２１０ａ、２１１ａに記録するときに一緒に記録し、また、コピー制御情報、並びに、コンテンツ鍵（もしくは、第１コンテンツ鍵、第２コンテンツ鍵）を、それぞれ、コピー制御情報記録部２０４、２０４ａ、並びに、コンテンツ鍵記録部２０６、２０６ａ１、２０６ａ２に記録するときに、前記コンテンツ識別情報を一緒に記録する構成としてもよい。これにより、例えば、ある第２暗号化コンテンツを可搬媒体１０４ａに移動するとき、そのコンテンツ識別情報と同じコンテンツ識別情報を有するコピー制御情報、並びにコンテンツ鍵（もしくは、第１コンテンツ鍵、第２コンテンツ鍵）を、コピー制御情報記録部２０４、２０４ａ、並びに、コンテンツ鍵記録部２０６、２０６ａ１、２０６ａ２より見出すことが可能となる。

【０１５７】

（１４）上記実施の形態１、及び上記実施の形態２では、コンテンツは外部のコンテンツ供給装置により供給される構成としたが、本発明はその構成に限定されるものではない。例えば、記録再生装置に挿入された記録媒体からコンテンツを読み出す構成であってもよい。

【産業上の利用可能性】

【０１５８】

本発明にかかる著作権保護システムは、コンテンツの移動元の記録再生装置が、コンテンツの移動時に当該コンテンツを復号するための鍵も合わせて移動させることにより、記録再生装置内のコンテンツを消去することなく利用不可状態にすることができ、移動したコンテンツを再び当該記録再生装置へ戻す場合に、前記復号するための鍵を元に戻す（移動させる）ことにより、元々の高画質コンテンツを復元可能（利用可能）にできるという効果を有し、ユーザ利便性を損なわない著作権保護システムの実現において有用である。

【図面の簡単な説明】

【０１５９】

【図１】本発明に係る著作権保護システムの全体構成を示すブロック図

【図２】本発明の実施の形態１における機能ブロック図

【図３】本発明の実施の形態１における記録再生装置にコンテンツを記録する際の動作フロー図

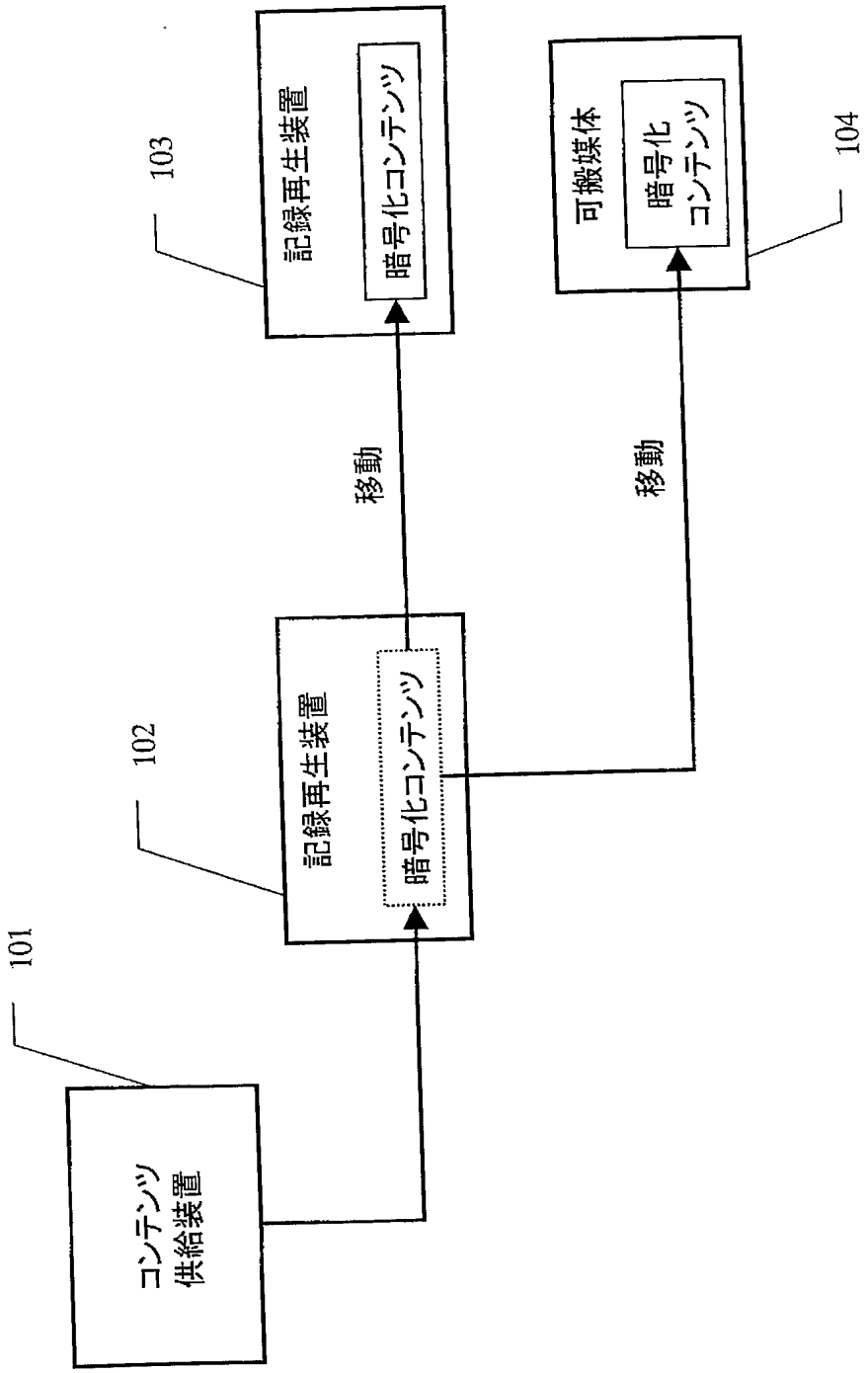
【図４】本発明の実施の形態１における記録再生装置から可搬媒体へコンテンツを移

動させる際の動作フロー図
【図５】本発明の実施の形態１における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図
【図６】本発明の実施の形態１における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図
【図７】本発明の実施の形態１における可搬媒体から記録再生装置へコンテンツを移動させる際の動作フロー図
【図８】本発明の実施の形態１における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図
【図９】本発明の実施の形態１における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図
【図１０】本発明の実施の形態１における記録再生装置に記録したコンテンツを再生する際の動作フロー図
【図１１】本発明の実施の形態１における機能ブロック図
【図１２】本発明の実施の形態２における記録再生装置にコンテンツを記録する際の動作フロー図
【図１３】本発明の実施の形態２における記録再生装置から可搬媒体へコンテンツを移動させる際の動作フロー図
【図１４】本発明の実施の形態２における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図
【図１５】本発明の実施の形態２における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図
【図１６】本発明の実施の形態２における可搬媒体から記録再生装置へコンテンツを移動させる際の動作フロー図
【図１７】本発明の実施の形態２における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図
【図１８】本発明の実施の形態２における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図
【図１９】本発明の実施の形態２における記録再生装置に記録したコンテンツを再生する際の動作フロー図

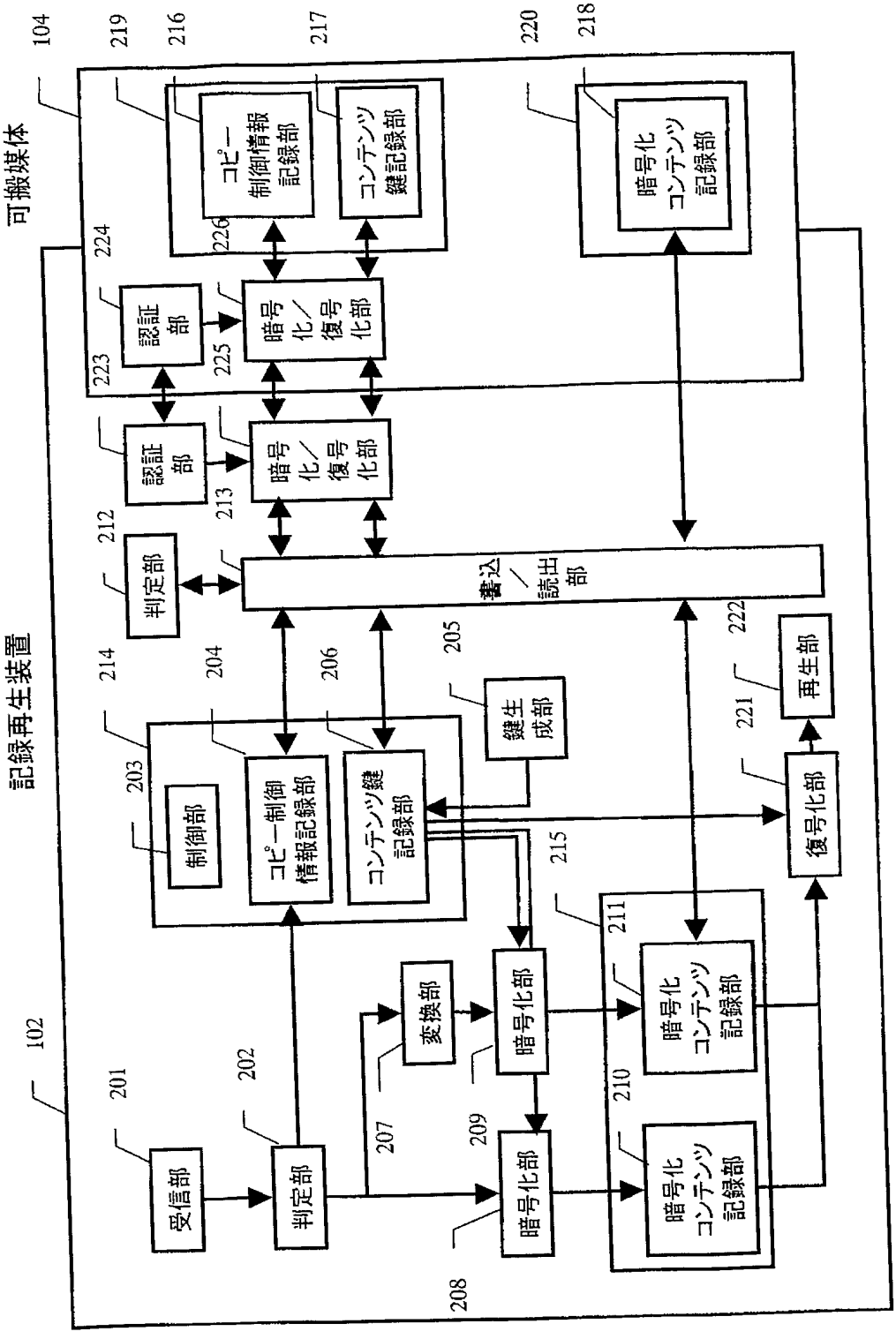
【符号の説明】
【０１６０】
１０１　　コンテンツ供給装置
１０２，１０２ａ　　記録再生装置
１０３　　記録再生装置
１０４，１０４ａ　　可搬媒体
２０１，２０１ａ　　受信部
２０２，２０２ａ　　判定部
２０３，２０３ａ　　制御部
２０４，２０４ａ，２１６，２１６ａ　　コピー制御情報記録部
２０５，２０５ａ　　鍵生成部
２０６，２０６ａ１，２０６ａ２，２１７，２１７ａ　　コンテンツ鍵記録部
２０７，２０７ａ　　変換部
２０８，２０８ａ，２０９，２０９ａ　　暗号化部
２１０，２１０ａ，２１１，２１１ａ，２１８，２１８ａ　　暗号化コンテンツ記録部
２１２，２１２ａ　　判定部
２１３，２１３ａ　　書込／読出部
２１４，２１４ａ，２１５，２１５ａ，２１９，２１９ａ，２２０，２２０ａ　　領域
２２１，２２１ａ　　復号化部
２２２，２２２ａ　　再生部

２２３，２２３ａ，２２４，２２４ａ　認証部
２２５，２２５ａ，２２６，２２６ａ　暗号化／復号化部

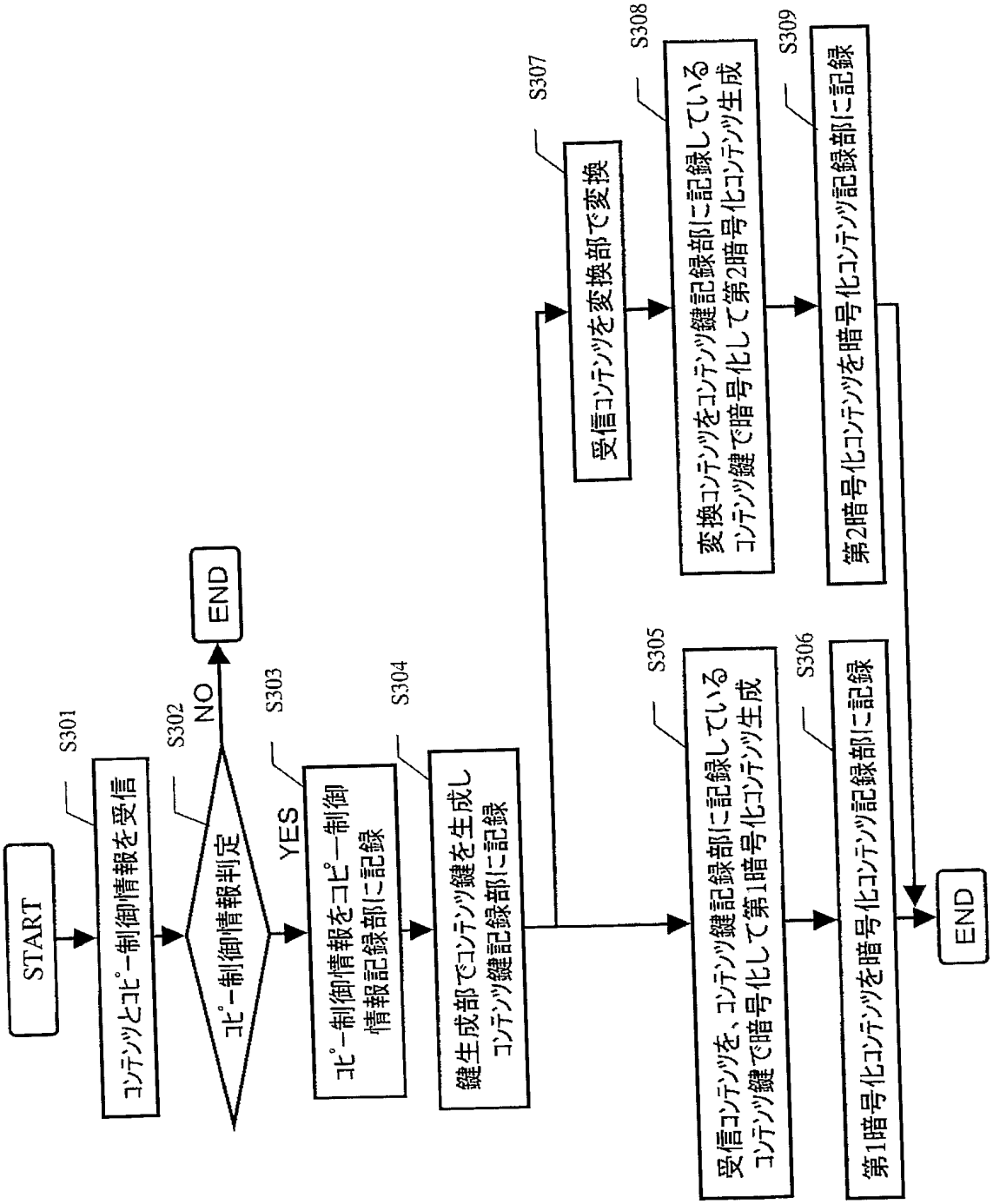
【書類名】図面
【図１】


101
コンテンツ
供給装置
102
記録再生装置
暗号化コンテンツ
移動
103
記録再生装置
暗号化コンテンツ
移動
104
可搬媒体
暗号化
コンテンツ

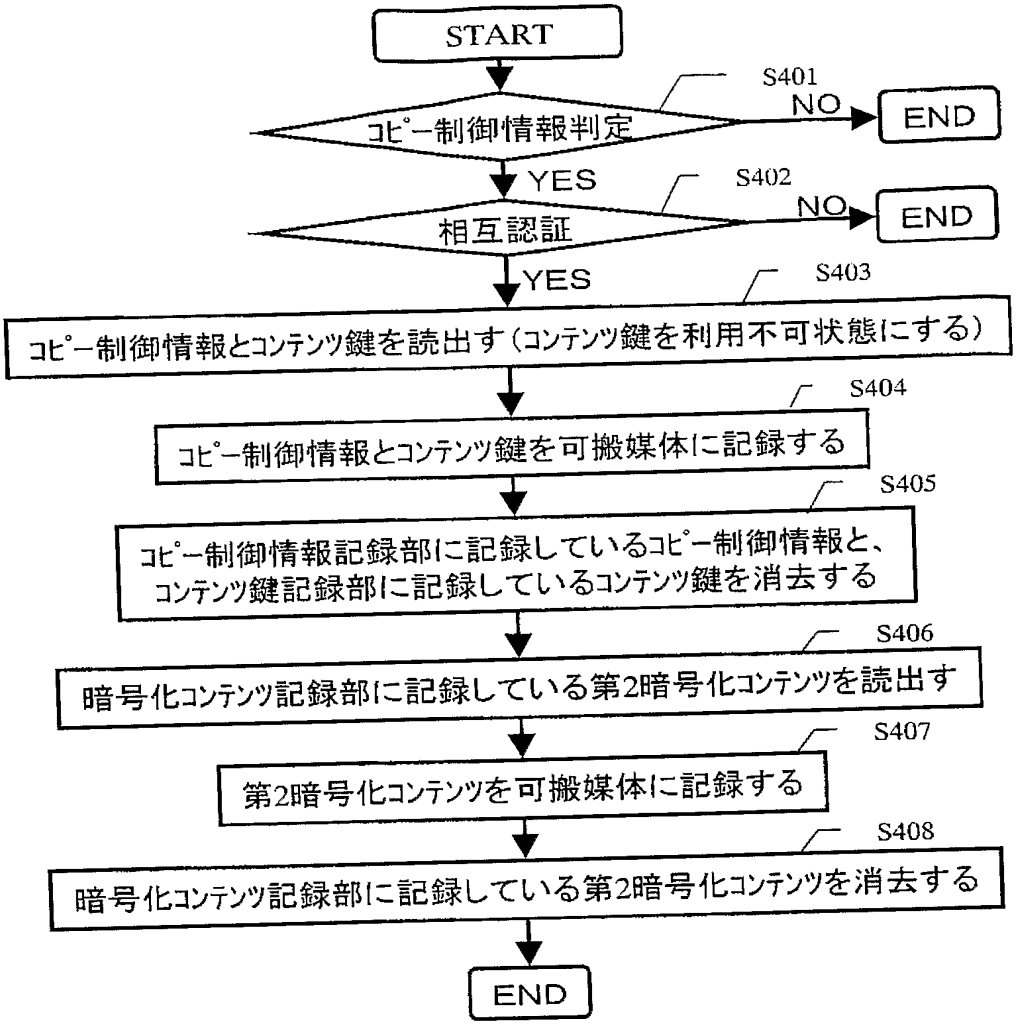
【図２】


記録再生装置
102
可搬媒体
104
受信部
201
判定部
202
制御部
203
コピー制御情報記録部
204
コンテンツ鍵記録部
206
鍵生成部
205
判定部
214
書込／読出部
212
認証部
213
暗号化／復号化部
認証部
223
暗号化／復号化部
225
コピー制御情報記録部
226
コンテンツ鍵記録部
224
暗号化コンテンツ記録部
220
218
219
216
217
再生部
222
221
復号化部
変換部
207
暗号化部
209
暗号化部
208
暗号化コンテンツ記録部
210
暗号化コンテンツ記録部
211
215

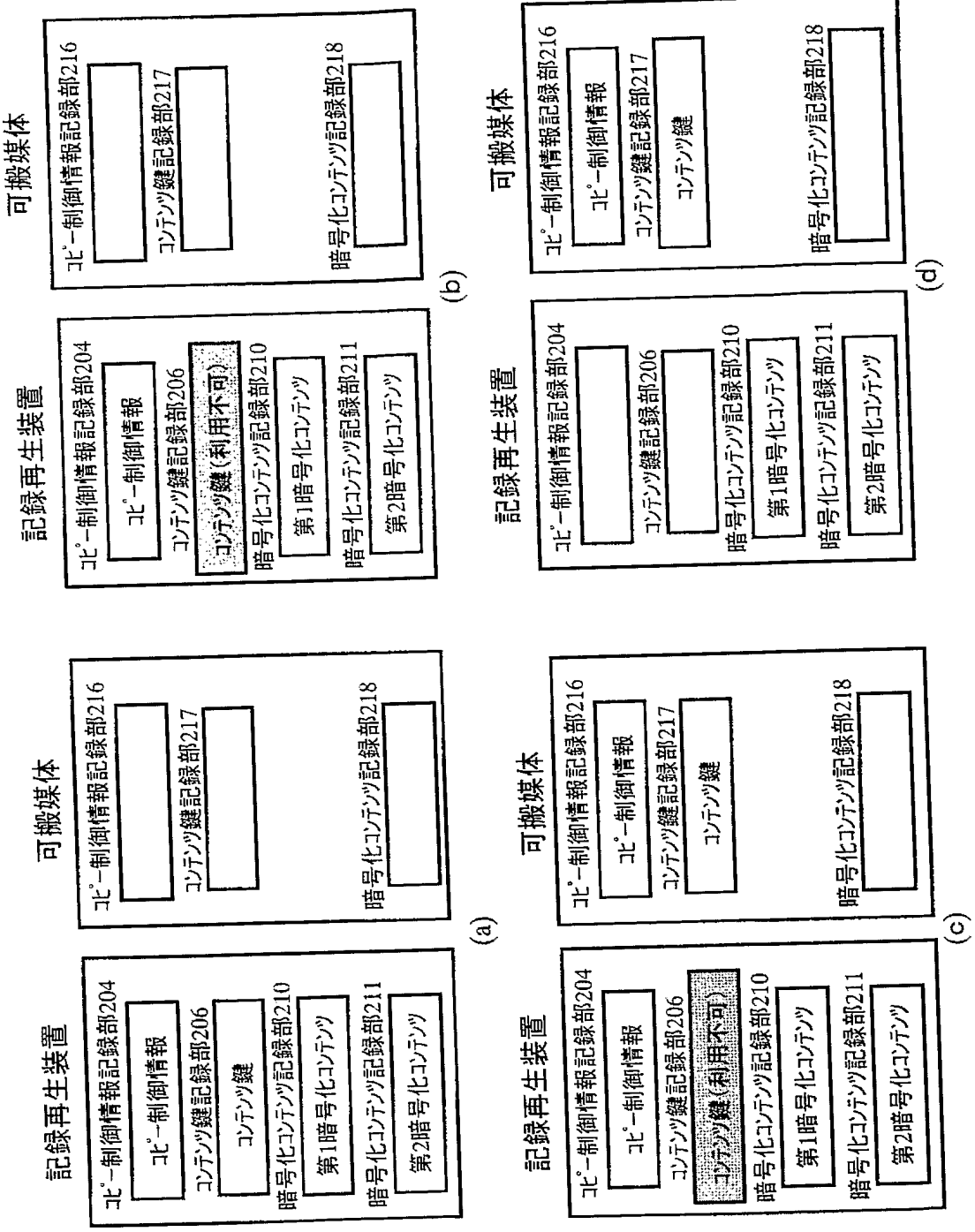
【図３】


START
S301
コンテンツとコピー制御情報を受信
S302
コピー制御情報判定
NO
END
YES
S303
コピー制御情報をコピー制御情報記録部に記録
S304
鍵生成部でコンテンツ鍵を生成しコンテンツ鍵記録部に記録
S305
受信コンテンツを、コンテンツ鍵記録部に記録しているコンテンツ鍵で暗号化して第1暗号化コンテンツ生成
S306
第1暗号化コンテンツを暗号化コンテンツ記録部に記録
S307
受信コンテンツを変換部で変換
S308
変換コンテンツをコンテンツ鍵記録部に記録しているコンテンツ鍵で暗号化して第2暗号化コンテンツ生成
S309
第2暗号化コンテンツを暗号化コンテンツ記録部に記録
END

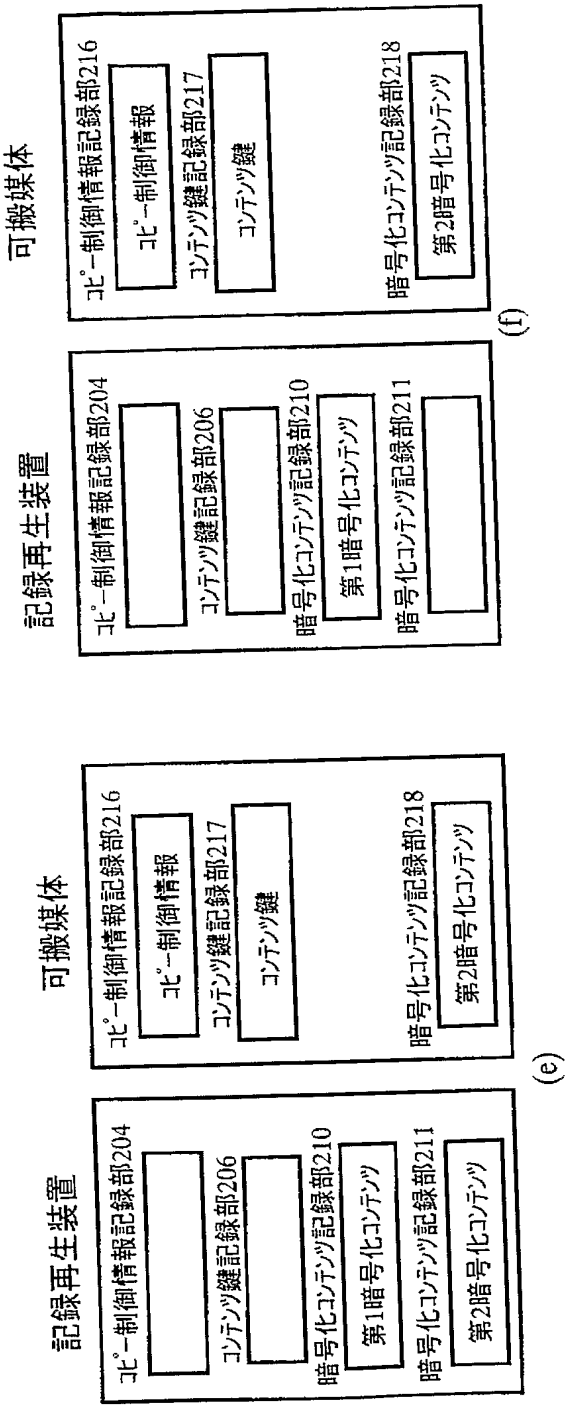
【図４】


START
S401
コピー制御情報判定
NO
END
YES
S402
相互認証
NO
END
YES
S403
コピー制御情報とコンテンツ鍵を読出す（コンテンツ鍵を利用不可状態にする）
S404
コピー制御情報とコンテンツ鍵を可搬媒体に記録する
S405
コピー制御情報記録部に記録しているコピー制御情報と、
コンテンツ鍵記録部に記録しているコンテンツ鍵を消去する
S406
暗号化コンテンツ記録部に記録している第2暗号化コンテンツを読出す
S407
第2暗号化コンテンツを可搬媒体に記録する
S408
暗号化コンテンツ記録部に記録している第2暗号化コンテンツを消去する
END

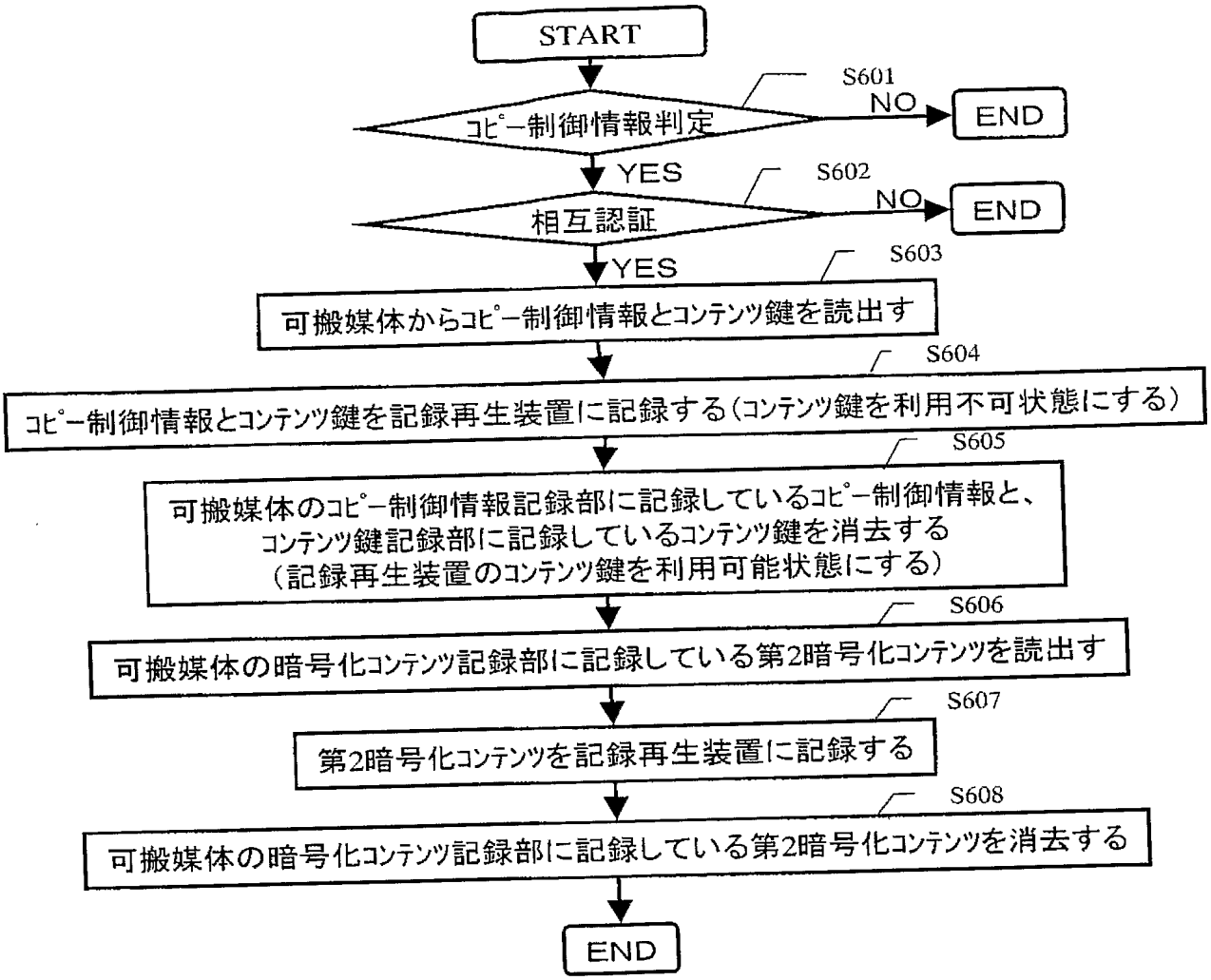
【図５】


記録再生装置
コピー制御情報記録部204
コピー制御情報
コンテンツ鍵記録部206
コンテンツ鍵
暗号化コンテンツ記録部210
第1暗号化コンテンツ
暗号化コンテンツ記録部211
第2暗号化コンテンツ
可搬媒体
コピー制御情報記録部216
コンテンツ鍵記録部217
暗号化コンテンツ記録部218
(a)
コンテンツ鍵（利用不可）
(b)
(c)
(d)

【図６】


可搬媒体
記録再生装置
コピー制御情報記録部204
コンテンツ鍵記録部206
暗号化コンテンツ記録部210
第1暗号化コンテンツ
暗号化コンテンツ記録部211
第2暗号化コンテンツ
(e)
可搬媒体
記録再生装置
コピー制御情報記録部216
コピー制御情報
コンテンツ鍵記録部217
コンテンツ鍵
暗号化コンテンツ記録部218
第2暗号化コンテンツ
(f)

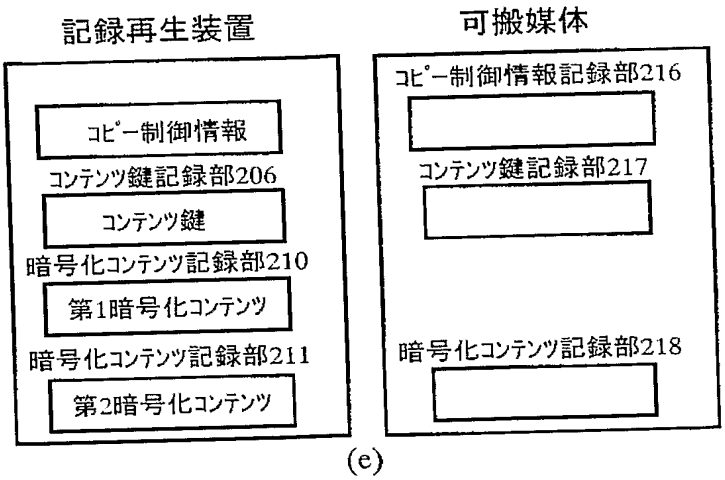
【図７】


START
S601
コピー制御情報判定
NO
END
YES
S602
相互認証
NO
END
YES
S603
可搬媒体からコピー制御情報とコンテンツ鍵を読出す
S604
コピー制御情報とコンテンツ鍵を記録再生装置に記録する(コンテンツ鍵を利用不可状態にする)
S605
可搬媒体のコピー制御情報記録部に記録しているコピー制御情報と、
コンテンツ鍵記録部に記録しているコンテンツ鍵を消去する
(記録再生装置のコンテンツ鍵を利用可能状態にする)
S606
可搬媒体の暗号化コンテンツ記録部に記録している第2暗号化コンテンツを読出す
S607
第2暗号化コンテンツを記録再生装置に記録する
S608
可搬媒体の暗号化コンテンツ記録部に記録している第2暗号化コンテンツを消去する
END

【図８】

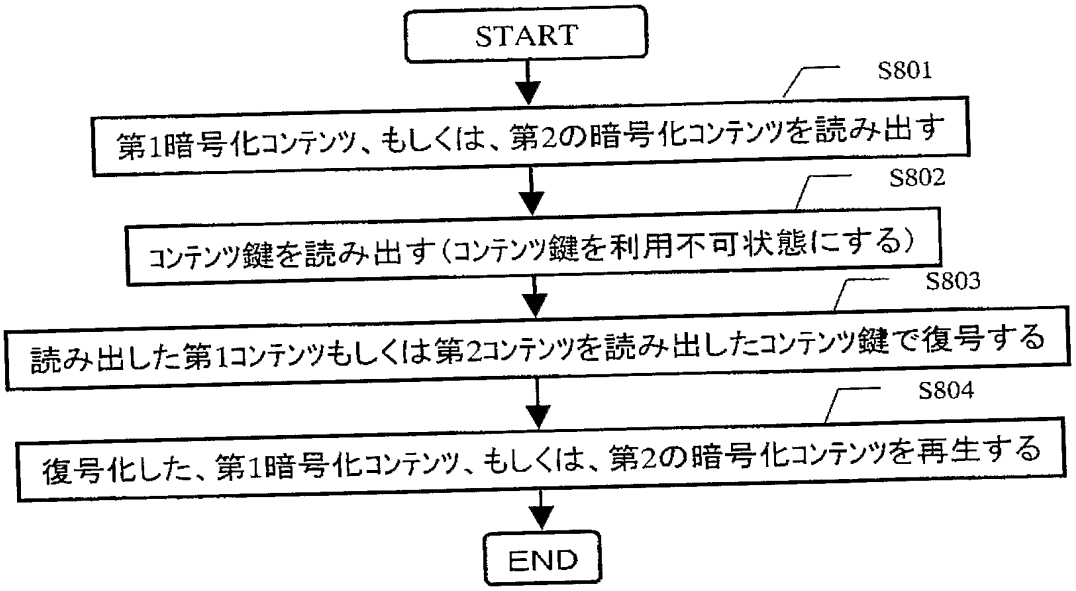
記録再生装置
可搬媒体
コピー制御情報記録部204
コンテンツ鍵記録部206
暗号化コンテンツ記録部210
第1暗号化コンテンツ
暗号化コンテンツ記録部211
コピー制御情報記録部216
コピー制御情報
コンテンツ鍵記録部217
コンテンツ鍵
暗号化コンテンツ記録部218
第2暗号化コンテンツ
(a)
記録再生装置
可搬媒体
コピー制御情報記録部204
コピー制御情報
コンテンツ鍵記録部206
コンテンツ鍵（利用不可）
暗号化コンテンツ記録部210
第1暗号化コンテンツ
暗号化コンテンツ記録部211
コピー制御情報記録部216
コピー制御情報
コンテンツ鍵記録部217
コンテンツ鍵
暗号化コンテンツ記録部218
第2暗号化コンテンツ
(b)
記録再生装置
可搬媒体
コピー制御情報
コンテンツ鍵記録部206
コンテンツ鍵
暗号化コンテンツ記録部210
第1暗号化コンテンツ
暗号化コンテンツ記録部211
コピー制御情報記録部216
コンテンツ鍵記録部217
暗号化コンテンツ記録部218
第2暗号化コンテンツ
(c)
記録再生装置
可搬媒体
コピー制御情報
コンテンツ鍵記録部206
コンテンツ鍵
暗号化コンテンツ記録部210
第1暗号化コンテンツ
暗号化コンテンツ記録部211
コピー制御情報記録部216
コンテンツ鍵記録部217
暗号化コンテンツ記録部218
第2暗号化コンテンツ
(d)

【図９】

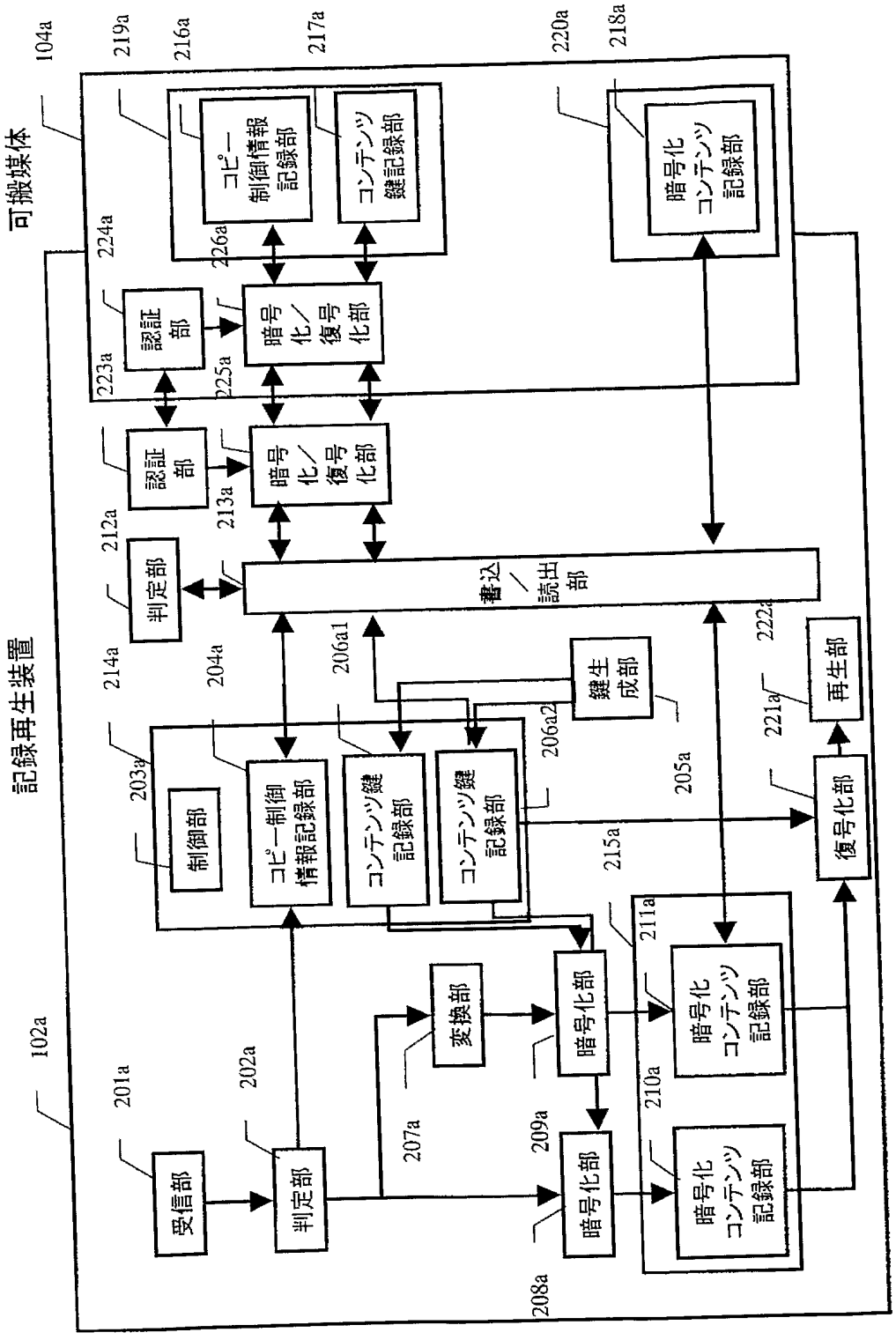

記録再生装置
コピー制御情報
コンテンツ鍵記録部206
コンテンツ鍵
暗号化コンテンツ記録部210
第1暗号化コンテンツ
暗号化コンテンツ記録部211
第2暗号化コンテンツ
可搬媒体
コピー制御情報記録部216
コンテンツ鍵記録部217
暗号化コンテンツ記録部218

(e)

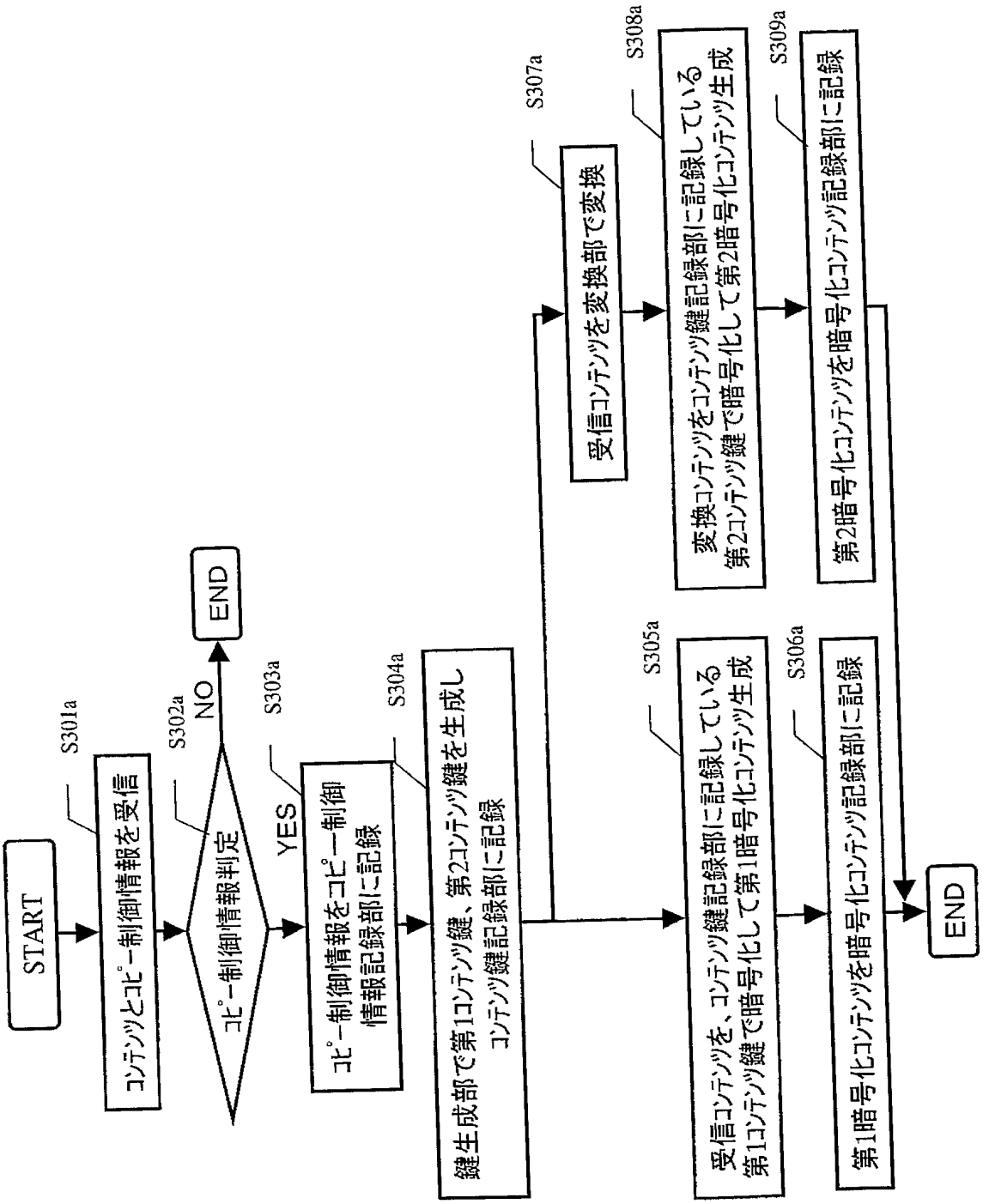
【図１０】


START
S801
第1暗号化コンテンツ、もしくは、第2の暗号化コンテンツを読み出す
S802
コンテンツ鍵を読み出す（コンテンツ鍵を利用不可状態にする）
S803
読み出した第1コンテンツもしくは第2コンテンツを読み出したコンテンツ鍵で復号する
S804
復号化した、第1暗号化コンテンツ、もしくは、第2の暗号化コンテンツを再生する
END

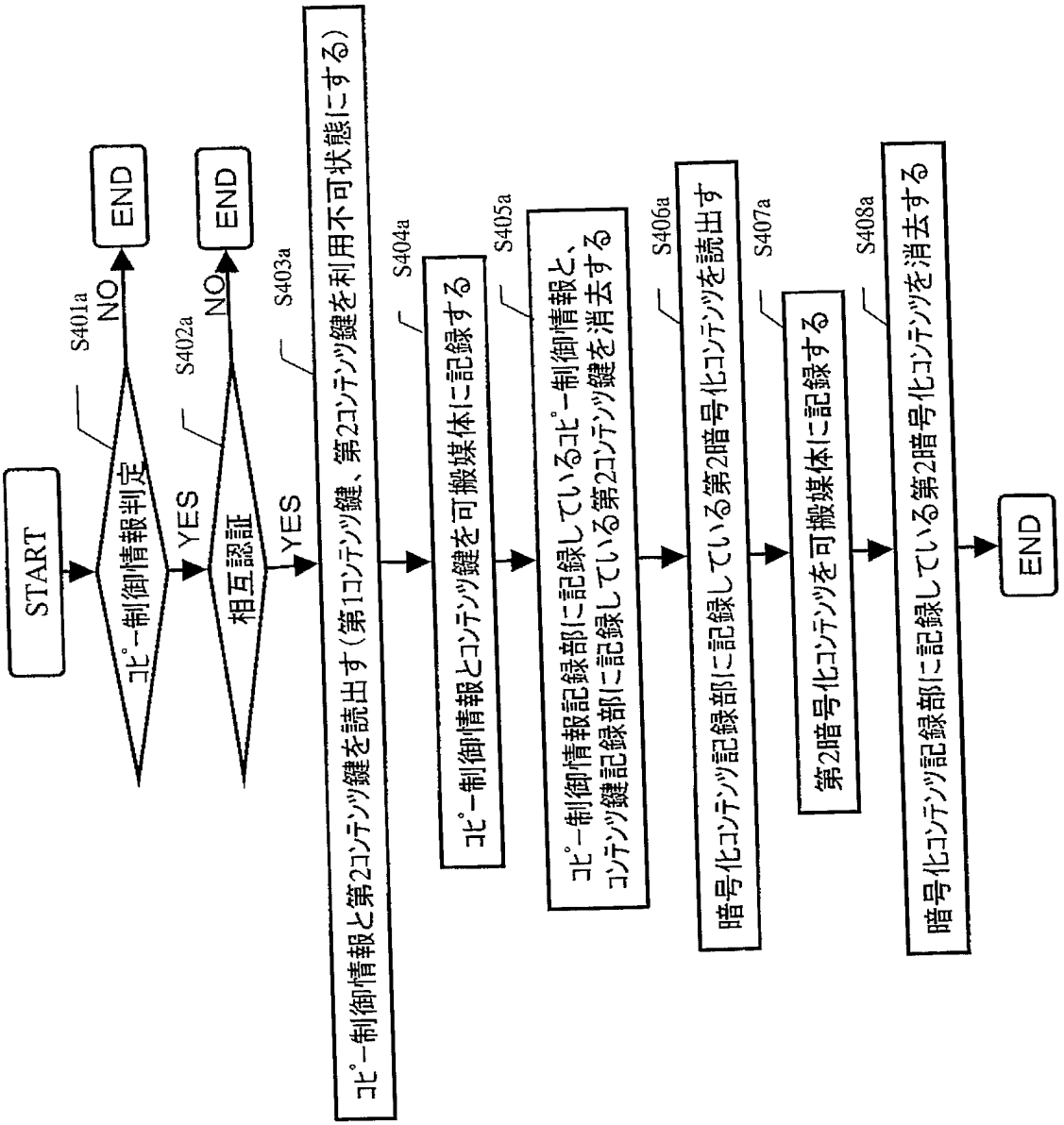
【図１１】


可搬媒体
104a
記録再生装置
102a
219a
216a
217a
220a
218a
224a
226a
コピー制御情報記録部
コンテンツ鍵記録部
暗号化コンテンツ記録部
223a
認証部
暗号化／復号化部
225a
212a
213a
判定部
書込／読出部
214a
204a
206a1
206a2
鍵生成部
222a
再生部
203a
制御部
コピー制御情報記録部
コンテンツ鍵記録部
コンテンツ鍵記録部
221a
205a
復号化部
215a
211a
201a
202a
変換部
暗号化部
暗号化コンテンツ記録部
受信部
判定部
207a
209a
210a
暗号化部
暗号化コンテンツ記録部
208a

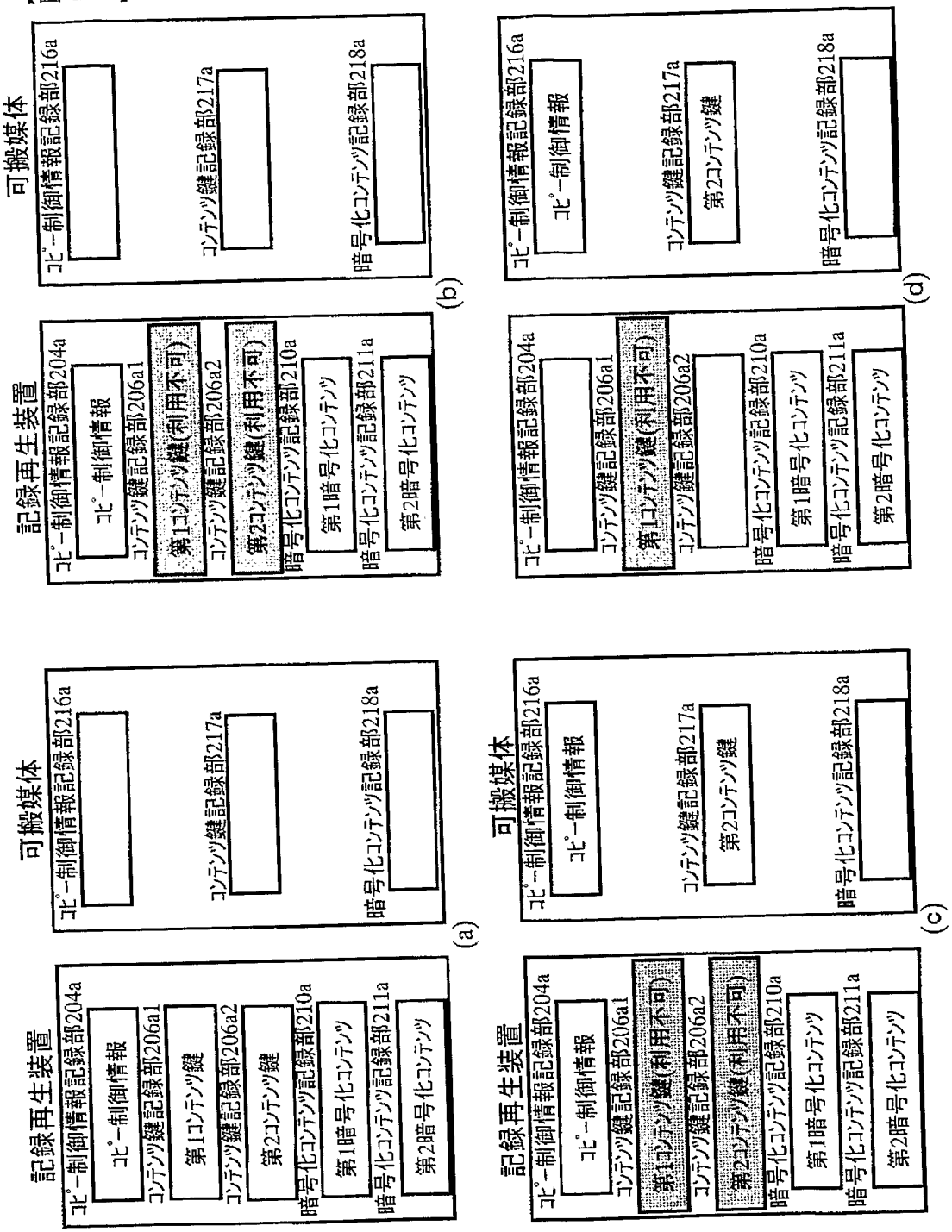
【図１２】


START
S301a
コンテンツとコピー制御情報を受信
S302a
コピー制御情報判定
NO
END
YES
S303a
コピー制御情報をコピー制御情報記録部に記録
S304a
鍵生成部で第1コンテンツ鍵、第2コンテンツ鍵を生成し
コンテンツ鍵記録部に記録
S305a
受信コンテンツを、コンテンツ鍵記録部に記録している
第1コンテンツ鍵で暗号化して第1暗号化コンテンツ生成
S306a
第1暗号化コンテンツを暗号化コンテンツ記録部に記録
S307a
受信コンテンツを変換部で変換
S308a
変換コンテンツをコンテンツ鍵記録部に記録している
第2コンテンツ鍵で暗号化して第2暗号化コンテンツ生成
S309a
第2暗号化コンテンツを暗号化コンテンツ記録部に記録
END

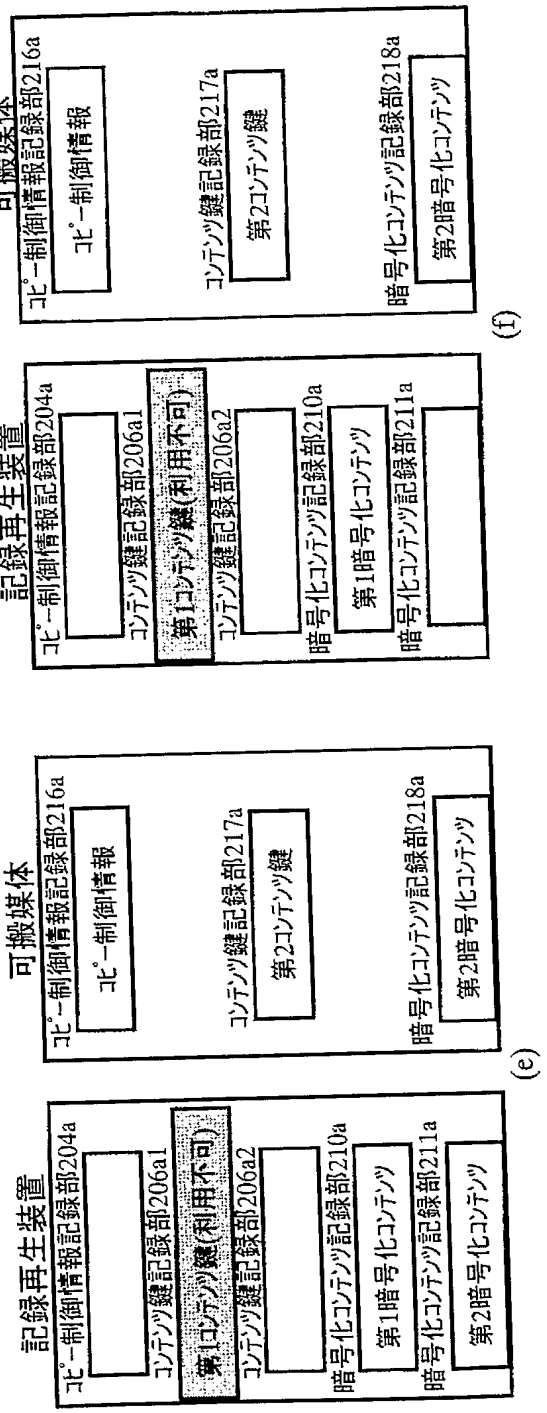
【図１３】


START
S401a
コピー制御情報判定
NO
END
YES
S402a
相互認証
NO
END
YES
S403a
コピー制御情報と第2コンテンツ鍵を読出す（第1コンテンツ鍵、第2コンテンツ鍵を利用不可状態にする）
S404a
コピー制御情報とコンテンツ鍵を可搬媒体に記録する
S405a
コピー制御情報記録部に記録しているコピー制御情報と、コンテンツ鍵記録部に記録している第2コンテンツ鍵を消去する
S406a
暗号化コンテンツ記録部に記録している第2暗号化コンテンツを読出す
S407a
第2暗号化コンテンツを可搬媒体に記録する
S408a
暗号化コンテンツ記録部に記録している第2暗号化コンテンツを消去する
END

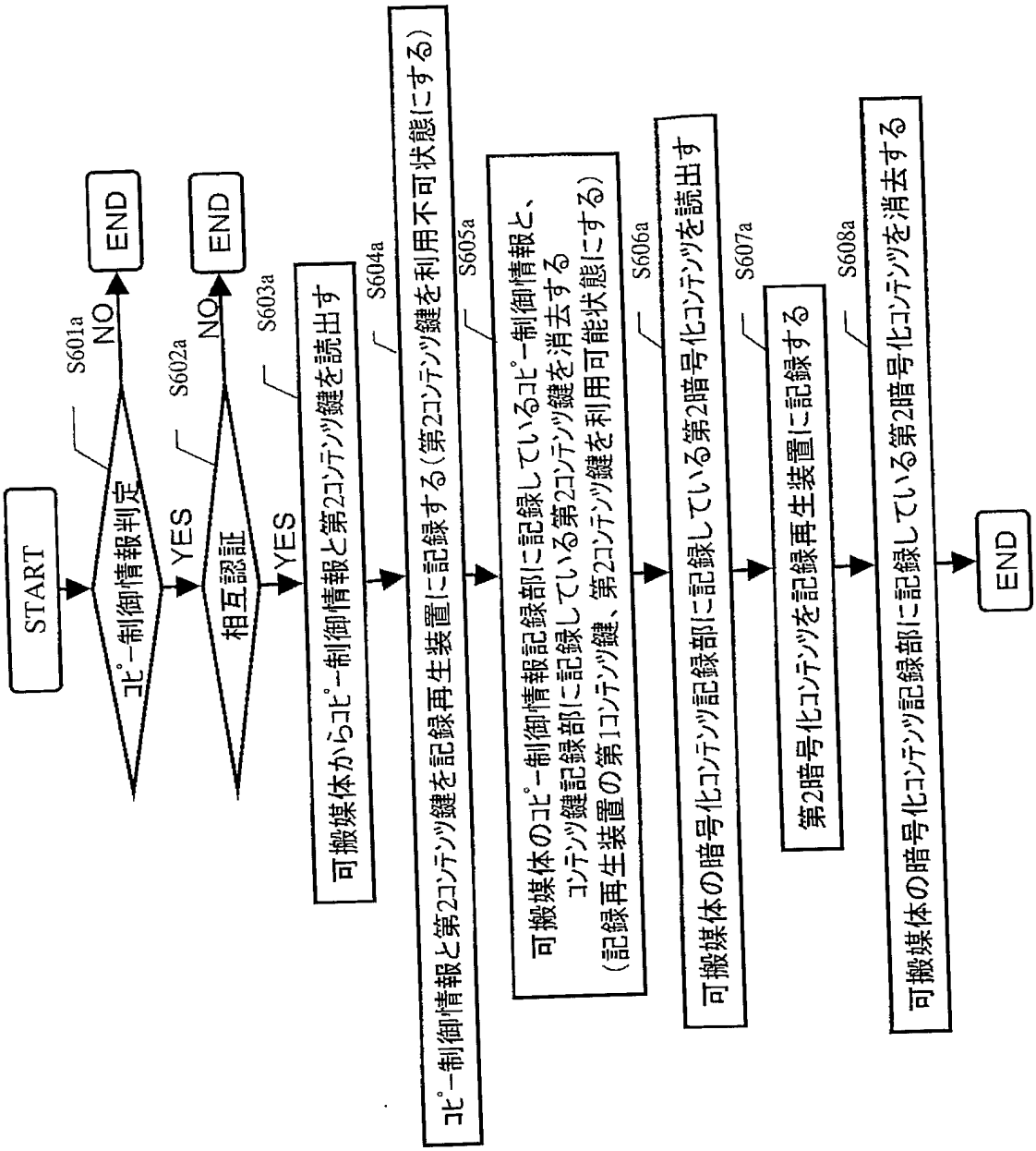
【図１４】


可搬媒体
記録再生装置
ｺﾋﾟｰ制御情報記録部216a
ｺﾋﾟｰ制御情報記録部204a
ｺﾋﾟｰ制御情報
コンテンツ鍵記録部206a1
第1コンテンツ鍵
コンテンツ鍵記録部206a2
第2コンテンツ鍵
暗号化コンテンツ記録部210a
第1暗号化コンテンツ
暗号化コンテンツ記録部211a
第2暗号化コンテンツ
コンテンツ鍵記録部217a
暗号化コンテンツ記録部218a
第1コンテンツ鍵(利用不可)
第2コンテンツ鍵(利用不可)
(a)
(b)
(c)
(d)

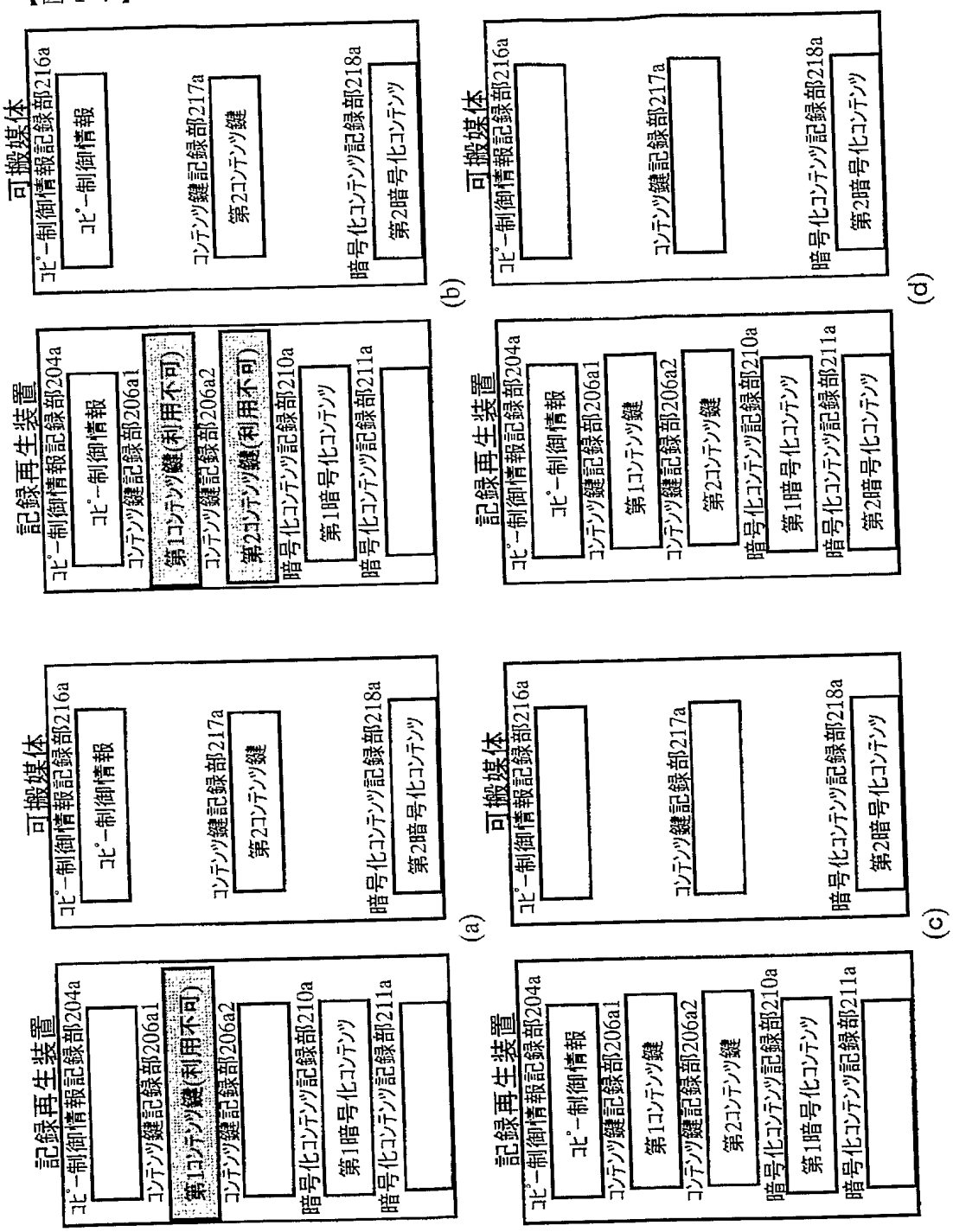
【図１５】


記録再生装置
ｺﾋﾟｰ制御情報記録部204a
コンテンツ鍵記録部206a1
第1コンテンツ鍵(利用不可)
コンテンツ鍵記録部206a2
暗号化コンテンツ記録部210a
第1暗号化コンテンツ
暗号化コンテンツ記録部211a
第2暗号化コンテンツ
(e)
可搬媒体
ｺﾋﾟｰ制御情報記録部216a
ｺﾋﾟｰ制御情報
コンテンツ鍵記録部217a
第2コンテンツ鍵
暗号化コンテンツ記録部218a
第2暗号化コンテンツ
記録再生装置
ｺﾋﾟｰ制御情報記録部204a
コンテンツ鍵記録部206a1
第1コンテンツ鍵(利用不可)
コンテンツ鍵記録部206a2
暗号化コンテンツ記録部210a
第1暗号化コンテンツ
暗号化コンテンツ記録部211a
(f)
可搬媒体
ｺﾋﾟｰ制御情報記録部216a
ｺﾋﾟｰ制御情報
コンテンツ鍵記録部217a
第2コンテンツ鍵
暗号化コンテンツ記録部218a
第2暗号化コンテンツ

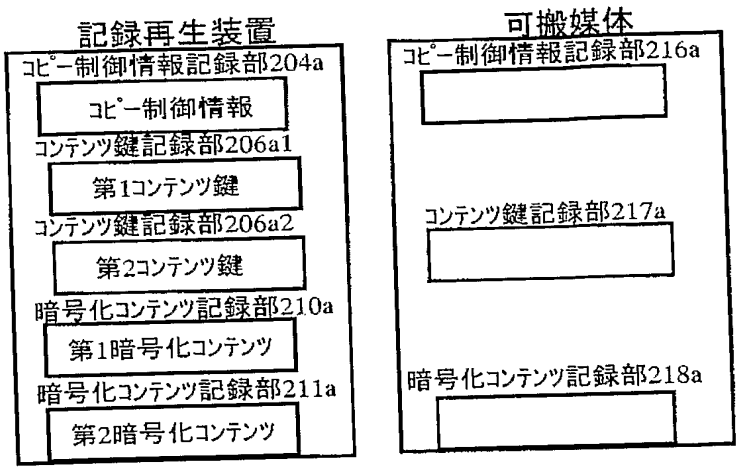
【図１６】


START
S601a
ｺﾋﾟｰ制御情報判定
NO
END
YES
S602a
相互認証
NO
END
YES
S603a
可搬媒体からｺﾋﾟｰ制御情報と第2ｺﾝﾃﾝﾂ鍵を読出す
S604a
ｺﾋﾟｰ制御情報と第2ｺﾝﾃﾝﾂ鍵を記録再生装置に記録する（第2ｺﾝﾃﾝﾂ鍵を利用不可状態にする）
S605a
可搬媒体のｺﾋﾟｰ制御情報記録部に記録しているｺﾋﾟｰ制御情報と、
ｺﾝﾃﾝﾂ鍵記録部に記録している第2ｺﾝﾃﾝﾂ鍵を消去する
（記録再生装置の第1ｺﾝﾃﾝﾂ鍵、第2ｺﾝﾃﾝﾂ鍵を利用可能状態にする）
S606a
可搬媒体の暗号化ｺﾝﾃﾝﾂ記録部に記録している第2暗号化ｺﾝﾃﾝﾂを読出す
S607a
第2暗号化ｺﾝﾃﾝﾂを記録再生装置に記録する
S608a
可搬媒体の暗号化ｺﾝﾃﾝﾂ記録部に記録している第2暗号化ｺﾝﾃﾝﾂを消去する
END

【図１７】

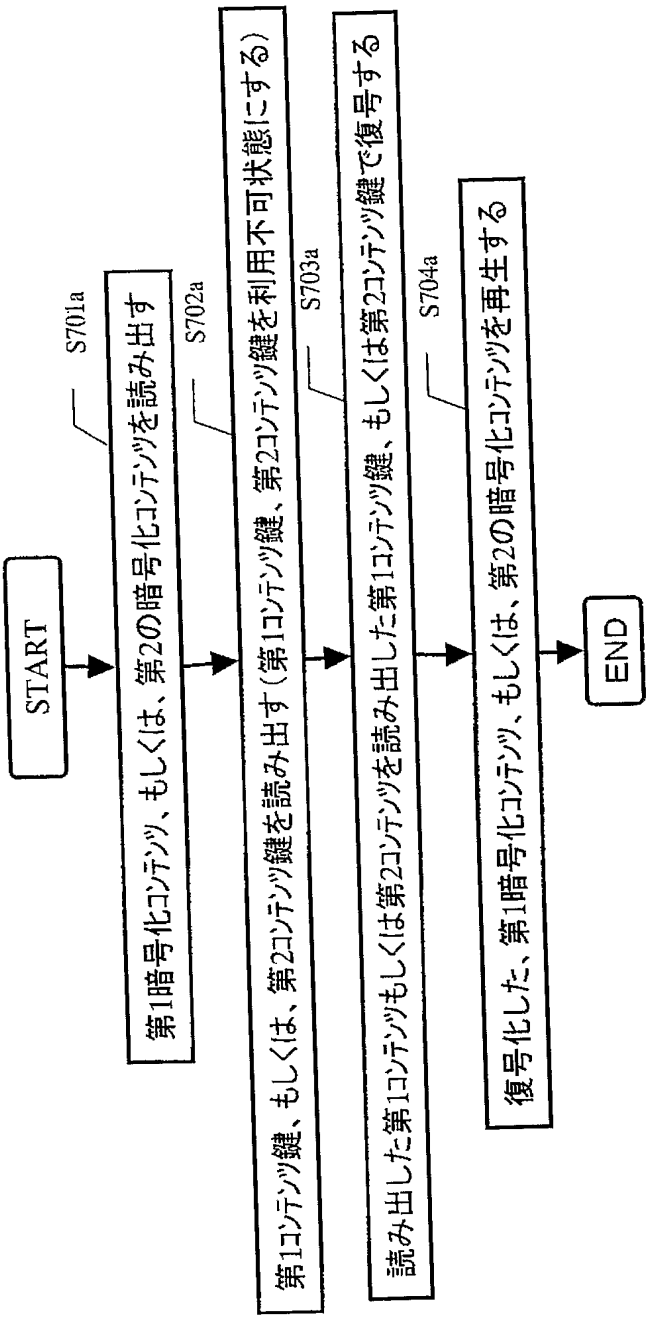

記録再生装置
ｺﾋﾟｰ制御情報記録部204a
ｺﾋﾟｰ制御情報
コンテンツ鍵記録部206a1
第1コンテンツ鍵(利用不可)
コンテンツ鍵記録部206a2
暗号化コンテンツ記録部210a
第1暗号化コンテンツ
暗号化コンテンツ記録部211a
可搬媒体
ｺﾋﾟｰ制御情報記録部216a
ｺﾋﾟｰ制御情報
コンテンツ鍵記録部217a
第2コンテンツ鍵
暗号化コンテンツ記録部218a
第2暗号化コンテンツ
(a)
(b)
(c)
(d)

【図１８】


記録再生装置
ｺﾋﾟｰ制御情報記録部204a
ｺﾋﾟｰ制御情報
ｺﾝﾃﾝﾂ鍵記録部206a1
第1ｺﾝﾃﾝﾂ鍵
ｺﾝﾃﾝﾂ鍵記録部206a2
第2ｺﾝﾃﾝﾂ鍵
暗号化ｺﾝﾃﾝﾂ記録部210a
第1暗号化ｺﾝﾃﾝﾂ
暗号化ｺﾝﾃﾝﾂ記録部211a
第2暗号化ｺﾝﾃﾝﾂ
可搬媒体
ｺﾋﾟｰ制御情報記録部216a
ｺﾝﾃﾝﾂ鍵記録部217a
暗号化ｺﾝﾃﾝﾂ記録部218a

(e)

【図１９】


START
S701a
第1暗号化コンテンツ、もしくは、第2の暗号化コンテンツを読み出す
S702a
第1コンテンツ鍵、もしくは、第2コンテンツ鍵を読み出す（第1コンテンツ鍵、第2コンテンツ鍵を利用不可状態にする）
S703a
読み出した第1コンテンツもしくは第2コンテンツを読み出した第1コンテンツ鍵、もしくは第2コンテンツ鍵で復号する
S704a
復号化した、第1暗号化コンテンツ、もしくは、第2の暗号化コンテンツを再生する
END

【書類名】要約書
【要約】
【課題】高画質コンテンツの画質を劣化させるなどしてサイズを小さく圧縮変換してからコンテンツの移動を行った場合、圧縮変換されたコンテンツだけが残ってしまう。
【解決手段】記録再生装置は、高画質コンテンツと圧縮変換したコンテンツを、それぞれ同じコンテンツ鍵で暗号化し暗号化コンテンツ記録部に記録するとともに、コンテンツ鍵をコンテンツ鍵記録部に記録する。記録再生装置から可搬媒体への移動処理時には、コンテンツ鍵記録部に記録したコンテンツ鍵をメモリカードのコンテンツ鍵記録部に記録すると同時に記録再生装置のコンテンツ鍵記録部から消去する。可搬媒体から記録再生装置への移動処理時には、メモリカードのコンテンツ鍵記録部に記録したコンテンツ鍵を、記録再生装置のコンテンツ鍵記録部に記録すると同時に、可搬媒体のコンテンツ鍵記録部から消去する。
【選択図】図２

特願２００４－１２５１９６

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社